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-122 002.
www.telenor.in

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

25 July 2016

Shri A.Robert Jerard Ravi
Advisor (QoS)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawahar Lal Nehru Marg
New Delhi 110002

Subject: Consultation Paper on Cloud Computing

Dear Sir,

This is with reference to the above referred TRAI consultation paper dated 10th June 2016 and press release no. 64/2016. In this regard, please find enclosed herewith 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**

(Pankaj Sharma)
Chief Corporate Affairs Officer

Encl: a.a

Registered Office
Unit No. 902, 9th floor, Le Meridian,
Commercial Tower, Windsor Place, New Delhi-110001
CIN: U64200DL2012PTC231991

Telenor (India) Response to TRAI Consultation Paper on Cloud Computing (dated 10 June 2016)

Preamble

In India, Cloud computing is at a nascent stage and will likely to get more traction for cloud transition in next 2-3 years. The National Telecom Policy 2012 has outlined the need of cloud computing and what all new policy initiatives and/or changes required in existing regulations to enable favourable ecosystem. TRAI vide this consultation paper has dealt comprehensively on all aspects important for the growth of cloud computing services in India. TRAI has raised various issues seeking views of stakeholders in order to put together the regulatory framework for cloud services. However, we believe that since the cloud services provided to different users are being offered as customized solution basis their business requirements and hence there is no requirement of regulatory intervention at this point of time. The concerns and issues should be mutually dealt by users and service providers of cloud services through well defined service level agreement.

Cloud Computing brings innovation, higher operational efficiency and economies of scale

Cloud computing is a tremendous innovation in the digital landscape that has changed the way IT solutions are delivered and how end-users put them to use. Cloud computing is set to transform how we do business and how we move up in the digital value chain. The cloud computing has enabled service providers by installing infrastructure / hosting server at one location and offering services across locations globally at faster pace thereby achieving economies of scale and operational efficiency. This has resulted into quick adoption of applications/ digital services and making them popular globally.

The cloud computing services are becoming important and will play a critical role in the success of the Digital India and smart city programs of the Government. Various Sectors/ Organizations see this as an opportunity to serve their customers digitally covering wide range of products / services ï Mobile financial services (digital transactions), M2M, IOT, m-Health, M-Agriculture, M-education, Govt. benefit transfer schemes, insurance etc.

Cloud Computing is purely an IT infrastructure

Cloud Computing is simply the delivery of on demand IT resources ï everything from applications to data centers over the internet on a pay-for-use basis[1] available for the organizations. TRAI has itself stated that the cloud computing is a shared pool of configurable computing resources including networks, servers, storage, applications and services that can be rapidly provisioned. Cloud computing is offering immense benefits to both provider and user. It enables better performance of applications/ software coupled with greater scalability and flexibility to manage IT operations in more economical manner. Thus, the cloud computing purely falls under IT infrastructure domain and any regulatory intervention enforcing specific rules is not desirable.

Restrictive regulations are not desirable for adoption and growth of cloud computing

TRAI vide this paper has suggested various provisions/ measures imperative for the overall growth and faster adoption of cloud computing in India. Some of them are - data control,

[1] https://www.ibm.com/cloud-computing/what-is-cloud-computing

interoperability, QoS, re-verification of billing and metering provisions, customer complaints and grievances mechanism, cloud security, cross border data transfer, physical location of data server etc. We are of the view that highly restrictive regulations will stifle innovation and impact the growth of cloud computing services and are not desirable. Instead, a light touch regulatory approach supported by standards, guidelines and template SLAs is recommended.

Key Submissions:

- Technology is fast changing and any stringent and specific regulation would hinder innovation and competitiveness with the ultimate impact on end users restricting them to reap full benefits of cloud services. Thus, specific regulation mandating control on data over cloud services is not desirable. Instead, voluntary framework and standards should be put in place to promote the cloud services

- Cloud interoperability and standardization have huge impact on the cloud adoption and usage. Relevant clauses in Service Level Agreement (SLA) and architectural decision factors as suggested in our response will act as an enabler without any regulatory intervention.

- Cloud services are provided as customized solution basis business requirements of different cloud users. Therefore, prescribing specific QoS parameters and their benchmarks may not be relevant to all users. This should be left to the cloud provider and user to decide mutually within the SLA.

- Billing and metering provisions for re-verifications differs from one user to another. Flexibility should be there for cloud users to select any combination of mechanisms suggested in our response.

- No need for any specific regulatory mechanism for handling customer complaints and grievances. Depending upon the nature of complaint and grievances, existing regulatory framework is adequate to handle the same.

- Technology neutral regulatory framework supported with voluntary code of practice, guidelines, industrial standards and modal contractual clauses is essential for ensuring security of cloud services. However, any over regulation will lead to increased barrier of entries, deterrent to foreign investments and increased cost in the provision of services.

- Effective jurisdiction needs to be established to enforce relevant regulations. The cross-border data transfer should be regulated instead of imposing blanket ban to fully harness the benefits of cloud computing. Government may publish list of countries where cross border data can be hosted similar to EU regulation.

- As suggested in the paper, alternatives of mandating hosting of data in India should be considered instead of emphasizing for physical location of data servers in India. The choice of locations for hosting data should be left to the cloud service provider.

- We support the proposed tax subsidies to promote cloud services in India.

In conclusion the cloud services are IT infrastructure and should continue to be governed under the IT Act, relevant changes may be made (section 4, 5), the rights of Individuals should be protected through legislative process (section 5.4) and modal contractual clauses should be defined for SLA and dispute resolution. Standards based approach for technical issues (section 6, 10) is our recommendation.

Question wise response:

Question 1: What are the paradigms of cost benefit analysis especially in terms of -

a. accelerating the design and roll out of services
b. Promotion of social networking, participative governance and e-commerce.
c. Expansion of new services.
d. Any other items or technologies. Please support your views with relevant data.

Response:

As highlighted by TRAI in this paper, in India, Cloud Computing offers huge potential for industries to grow and is opening up new windows of opportunities across multiple sectors. Various industries / corporate have started availing benefits of cloud services to get better performance of applications/ software coupled with greater scalability and flexibility to manage their IT operations in more economical manner.

The virtualisation is a first step towards moving to cloud which provides scalable and agile solutions which in turn results in:

- flexible capabilities to deal with demands
- reduced cost (resources such as personnel, hardware and infrastructure are leveraged externally)
- improved operational efficiency resulting in faster delivery and reduced cost for product creation and delivery, and improved innovation.

Because of these key benefits brought by cloud, it has been generally seen as a key enabler that assists organizations in delivering prompt, agile and innovative services to customers. In an environment where many entities are adopting cloud solutions, utility of cloud services is not only essential in keeping up with the consumers, but also keeping up with the markets and competitors.

In general, cloud services brings enormous benefits for organisation, however cost saving purely depends upon the needs of IT infrastructure including computing and storage, type of applications required to be run, kind of data to be stored on the cloud, availability of existing hardware / software etc. In our view, the cost benefit analysis of cloud services for the organisation is essential prior to investing in IT infrastructure and instrumental in helping to decide optimal IT solution with minimum CAPEX and OPEX requirements. Further data elaborating specifically the cost reduction in IT budget of an organization is outlined in our response in Question 2.

Question 2: Please indicate with details how the economies of scale in the cloud will help cost reduction in the IT budget of an organisation?

Response:
There are several reasons for organisations to shift from traditional IT infrastructure to Cloud computing. One of the most cited benefit is the economics of the Cloud. There are four distinct mechanisms[2] through which cost savings are generated for organisations:

- By lowering the opportunity cost of running technology
- By allowing for a shift from capital expenditure to operating expenditure
- By lowering the total cost of ownership of technology
- By giving organisations the ability to add business value by renewed focus on core activities.

2.1 80-20 rule

The 80-20 rule is often used within organizations to illustrate the large effects that small variables can have. The most well known use of the rule is the sales 80-20 rule which says that 80% of revenue for a business is derived from 20% of customers. Information Technology has its own series of 80-20 rules. Gartner has estimates that IT maintenance accounts for around 80% of total IT expenditure. When we look at organizations running their own data centre infrastructure, and extend Gartnerôs findings, we hypothesize that only 20% of the time and effort that goes into running applications, where all business value is concentrated, is actually concerned with running those applications themselves. The rest of 80% of time and cost is associated with core technology deployment, managing operating systems & servers, and running data centres.

Cloud Computing is a force that helps flip this ratio and gives IT departments the ability to spend 80% of their time on core business processes, like business application design. Itôs for this reason, the ability to go from 20% of time and money dedicated to core business processes to 80%, that the economics of Cloud Computing is so compelling.

Thus, cloud computing is an important tool for bringing economies of scale and economic benefits for the organisations by moving their IT infrastructure to the cloud i.e. a move to the Cloud can make the difference between an organization being 20% efficient, and one being 80% efficient.

2.2 Economies of Scale

The benefits of how economies of scale in the cloud will help cost reduction in the IT budget of an organization have been outlined in section 2.14 of the Consultation Paper, and Telenor agreed with the analysis.

In general, the scalability, resource pooling modal of cloud enabled savings on infrastructure and operational expenditure, and reduced resource redundancies whilst increasing resiliency to deal with increased demands. Many independent research have shown that cloud technology can save companies up to 10-20% of their annual IT budgets due to achieving

[2] *Loudonomics: The Economics of Cloud Computing authored by Ben Kepes as a part of cloudU series*

higher utilization rates (by widening capacities) and lower unit costs (by improving operational efficiency).

In practicality, there are several use cases that demonstrated and quantified the cost reduction for cloud adoption. In a whitepaper commissioned by the Australia Department of Broadband Communications and the Digital Economy, and written by independent consulting firm, KPMG, a 10 year modal of potential GDP impact of cloud computing adoption estimated a saving of 0.23% GDP at 75% adoption of cloud services, equivalent to up to 3.82 billion AUD savings on capital and operational costs[3]. In the example of a nation state, Hungary initiated cloud ventures in 2013, and it was reported that its IT budget has been reduced by 30% or HUF 30 billion as a result of the venture.

2.3 Economic Benefits

In addition to IT budget savings, there are also economic benefits that can be derived from an organizationõs adoption of cloud.

According to the statement published by the European Commission which adopted the õDigital Single Market[4] strategy, it states that that by maximizing the impact of cloud computing in the European economy, there is potential to add a cumulative total of ú449bn to the EU28 GDP (including the public sector), of which ú103bn in the year 2020. This would represent a share of 0.71% of total EU GDP. It was further estimated that between 2015 and 2020 approximately 303,000 new businesses could be created, particularly small and medium enterprises (SMEs), and almost 1 million jobs could be created during 2015-2020.

We believe that there are significant economic benefits to be gained from a move to Cloud Computing. These benefits accrue to a business in two distinct ways ï directly through reduced costs and indirectly by allowing for increased focus on core business functions.

Question 3: What parameters do the business enterprises focus on while selecting type of cloud service deployment model? How does a decision on such parameters differ for large business setups and SMEs?

Response:

The IT infrastructure needs of organisations / enterprises purely depends upon their business requirements which need to be analysed while selecting the type of cloud service deployment model.

3.1 Parameters on selection of cloud service deployment model

Some non-exclusive examples of the parameters that business enterprise focus on while selecting type of cloud service deployment modal include:

a. Cost effectiveness
b. Modularity

[3] *KPMG Whitepaper – modelling economic impact of cloud computing*
[4] *Budapest Business Journal, 2014 – Government Cloud: Reboot for Hungary's public sphere IT*

c. Scalability
d. Flexibility (agility)
e. Inter-operability (including portability) both internally and externally
f. Integration with the enterprise architecture (as-is and to-be) and existing legacy solutions
g. Sensitivity of data
h. Security capability
i. Location of the solution.

3.2 Decisions on parameters

Decision on such parameters would differ from entity to entity, and such distinction is not entirely only due to size of a company. Decisions on such parameters would differ largely depending on:

a. Resources including budget and hardware - different deployment modal would result in different assumption of security role and responsibilities, and require different level of infrastructure/ hardware
b. Skills and capabilities ï for example, private cloud environment requires more extensive IT management than public cloud
c. Risk appetite
d. Utility and demand
e. Nature of the business and purpose of service adoption

For example, a company specializing in VoIP may choose to select a cloud service based primarily on latency and availability over other parameters, even if it is more costly than other solutions. This can occur regardless of whether the company is of a large setup, or SMEs.

Question 4: How can a secure migration path may be prescribed so that migration and deployment from one cloud to another is facilitated without any glitches?

Response:

As rightly noted by TRAI in the paper, cloud interoperability and standardization have huge impact on the cloud adoption and usage. The vendor lock-in is a common issue encountered by end users with regards to cloud services. Due to factors such as lack of standardization and customized platforms for unique solution requirements, migration from one cloud to another is often challenging for end users.

Acknowledging the issue, European Commission has launched a call for tenders to study practices and insights relating to data and application portability when switching cloud service providers. The outcome of the report remains to be seen.

Possible measures and their relevance are case dependent, but some of the ways in which secure migration and deployment from one cloud to another may be prescribed include:

- Relevant service contract should include clauses like ï

- Data ownership definitions, setting relevant roles and responsibilities (*including, but not limited to data processing agreements, migration related roles and responsibilities*)
- Service termination / exit related conditions (*data export, migration related conditions, including but not limited to: format, interface, deadlines, secure deletion*)
- Existing cloud service provider not to use / analyse cloud user data (*especially in cases where end consumer data stored in the cloud related to their usage, behaviour pattern about a service / product offered in the market by cloud user*), in any manner, having ability to impact the market position of the cloud user in its market place.

- Architectural decision factors when engaging the service, including ï
  - Necessary level of modularity (*e.g., using micro services architecture, distributed system/ component architecture*)
  - Inter-operability (*including portability*) and integration e.g., containerization (e.g., Docker), middleware architecture layer for integration, using open standards (or de facto standards) ï including open and well documented APIs)

Question 5: What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?

Response:

A customer referred herein in this question is assumed to be any entity that secures services from cloud service providers, not limited only to end users such as individuals/ SMEs, but also entities and organizations that procure such services to enable effective business operation.

We do not support a specific mandatory regulatory regime that mandates control on data for cloud services. Technology is a fast changing field, and stringent and specific regulation would hinder innovation, with the ultimate impact being imposed on end users who are not able to reap the full benefits offered by cloud services. Besides, legislative processes are often lengthy and time-consuming, and any specific regulation of cloud providers may no longer be applicable when passed. These are the common challenges faced by regulators when intending to introduce prescriptive standards and regulations to regulate cloud services. A more elaborated rationale supporting minimal regulatory intervention is outlined in our responses given in Question 6, 10 and 12.

However, this is not equivalent to not introducing *any* mechanisms to facilitate procurement and use of such services. It is our view that an appropriate balance can be strike to protect consumersô rights, such as right to privacy, data protection (*as explained further in the remaining sections of this submission*) and data portability, whilst allowing technology to flourish and to benefit consumers.

In this response, it is of our view that data portability could be maintained through a two prong regulatory approach ï contractual framework for entities and organizations and legislative regulation for individuals.

5.1 Contractual framework for entities and organizations

A market that trades on goods and services should be able to operate in a manner where both the consumers (*in this instance, entities who procure cloud services*) and providers can achieve an equilibrium that protect each otherôs commercial interest. A challenge in enacting legislations to regulate data portability for entities that procure cloud services is the potential impact brought by the intervention (*as mentioned above, a more elaborated rationale supporting minimal regulatory intervention is outlined in our responses in Question 6, 10 and 12.*) For such entities, data portability would form part of their commercial interest. Therefore, right to data portability should be negotiated and enshrined through contractual agreements between the parties.

However, a concern that commonly arises on such approach to regulating a market is the bargaining power between the seller and the provider ï it could be easily foreseen that SMEs would not be able to negotiate contracts offered by large cloud service providers that are on a ñtake it or leave it basisò In practicality, we propose that this can be regulated through model contractual clauses, which should level the playing field and reduces the power imbalance between the parties.

In the EU, the European Commission has issued model contractual which can be utilized by entities including SMEs when transferring data outside of the EU. Such clauses mandate a minimum standard of protection that must be provided by a processor and require specific information on the means of protection, scope of processing etc to ensure a satisfactory level of data processing.

Leveraging from this framework, model contractual clauses could be drafted and used as a basis for negotiation between entities and service providers. This will ensure standardization across the utility of cloud services and ensure level playing field between the consumers and cloud providers.

The next issue is thus enforcement. How could the model contractual clauses be enforced? In our view, enforcement of the framework can be achieved not through regulation *specifically* on cloud services, but complementary regulatory and dispute resolution mechanisms.

5.2 Enforcement of the contractual framework

In EU, the adoption of the contractual framework has been widely accepted due to the regulation imposed by EU data protection directive and regulation on cross border data transfer.[5] We proposed that similar approach can be taken through embedment to the proposed ***Right to Privacy Bill***. Our view on cross border data transfer is further outlined in

[5] Under the *General Data Protection Regulation* (previously, directive), data can only be transferred out of the EU if same level of protection can be offered in the country to which the data is transferred to. Note that data processing is considered as data transfer under the regime, therefore, cloud service providers will also be captured.

our response to Question 14. Other reason to introduce a Right to Privacy Bill is also elaborated in below sections as well as response to Question 10 and 16.

Other alternative to the enactment of the Bill includes leveraging current legislations, such as amendments to the *Information Technology Act of 2000*.

The issue concerning the effective jurisdiction over the cloud providers (*in the event that such providers are not based in India*) for enforcement of such regulation is discussed in Question 14.

5.3 Complementary mechanisms

In certain jurisdictions, a broad interpretation of the consumer regulation, such as regulation of ómisleading and deceptive conductsôand óunfair trade practicesôcould be utilized to cover unfair conducts of the cloud service providers, in circumstances where misrepresentations had been made about the service.[6] Such representations may be that the data centre located in A, but in fact, it was located in B; or representation that the data was secured through a particular mean, but in fact no such security technology was in place.

An accessible dispute resolution mechanism should also be put in place to resolve contractual disputes concerning the relevant model contractual clauses. Inaccessible, costly and lengthy dispute resolution processes would create high barriers for SMEs in disputing the compliance of the contracts, thus rending the regime ineffective.

Through a combination of contractual, regulatory and dispute resolution mechanism framework, data portability for entities that procure cloud services could be better secured.

5.4 Legislative regulation

As opposed to entities, individuals need to be protected under a different regime. Conferring rights on individuals does not present the same challenge as conferring rights on entities, as the implication of hindering effectiveness and innovation of technology does not occur in an individual context. Further, the challenges of enforcing a similar contractual regime on individuals would raise questions such as to whom the contracts should be entered with (between end users and the cloud provider there may be different data processors), and entities are not capable of negotiating individual contracts with each individual end user.

Therefore, we are of the opinion that individuals should be empowered with legislative right to assume effective ownership of their data, including right to data transfer and portability. The recently introduced General Data Protection Regulation (GDPR) in the EU is an example legislation that provides the data subject a combination of different rights which confer effective ownership to their data, including:

a. Right to access and correction of data
b. Right to transfer of data, including consent requirement for transfer of data by data controller or processor

[6] In the US, the *US Federal Trade Commission Act has been used as a basis for action against technology providers who* engaged in óunfair and deceptive acts or practices affecting commerce.

c. Right to delete data.

It also imposes security obligations to the data processors, including intermediary entities such as cloud service providers. Through such legislative framework, end users can be empowered with right to data portability not only with cloud services (*which store and process their data),* but also other entities *(which control the flow of their data*).[7]

Again, this can be achieved through embedment to the proposed ***Right to Privacy Bill***, or through leveraging current legislations, such as amendments to the *Information Technology Act of 2000*.

The issue concerning the effective jurisdiction over the cloud providers (*in* the event that such providers are not based in India) for enforcement of such regulation is discussed in Question 14.

5.5 Monitoring and Enforcement

In order to ensure the compliance to the legislative regulation, and to resolve grievances or disputes to the model contractual clauses, there should be stringent monitoring of vendorsô conduct and enforcement of the relevant requirements.

Within the European Union, Data Protection Authorities are appointed to enforce privacy and data protection regulation. Under the GDPR, a penalty of up to 4% of an entityôs turnover will be imposed if contravention to the GDPR is found.

As such, an existing authority could be leveraged or new authorities appointed to monitor and enforce compliance to the regulatory provisions.

Question 6: What regulatory framework and standards should be put in place for ensuring interoperability of cloud services at various levels of implementation viz. abstraction, programming and orchestration layer?

Response:

Technology is fast changing and competitive. In such an environment, any particular restriction, even at the lowest level (e.g., related to programming language, platform and development methodology) can significantly impact innovation and competitiveness. Therefore, it is our view that voluntary, instead of mandatory framework and standards should be put in place to improve interoperability of cloud services.

Currently, there are already technology related standards and frameworks that can be leveraged to develop the voluntary framework and standards:

- Å TOGAF for general architecture framework
- Å SABSA or Zachmann for security architecture framework

[7] Data processors and data controllers can of course be the same entity in some circumstances.

- Relevant ISO, ETSI, GSMA, W3C or other standardization body provided material
- RFC and other similar industry best practices and recommendations
- Cloud Security Alliance standards and materials
- NIST and FIPS publications

The voluntary framework and standards can then be complemented by guidelines to the end users outlining factors to consider when choosing cloud services, including the various technical considerations during pre-selection of services.

Emphasis and guidance can be given to factors influencing interoperability of IaaS, PaaS and SaaS such as user interfaces, APIs, use of open technology for application environment, data format and application packaging formats. This will inform the users various factors to consider when negotiating with the cloud providers.

Question 7: What shall be the QoS parameters based on which the performance of different cloud service providers could be measured for different service models? The parameters essential and desirable and their respective benchmarks may be suggested.

Response:

The cloud services provided to different cloud users are being offered as customised solution basis their business requirements. The performance parameters related to quality of service are implemented and measured through SLAs (service level agreements) while subscribing the cloud services between cloud provider and cloud user.

As discussed in para 3 (d) of the consultation paper, different QoS parameters such as availability, response time and billing correctness can be used to measure performance of different cloud service providers. However, QoS parameters differ vastly depending on the solutions provided and the business priorities of the cloud users. For example, for provision of VoIP, latency would be an area of concern when engaging providers. For others, latency may not be a QoS parameter used to measure their providers.

In view of above, it is recommended that since cloud solutions are purely tailor-made to meet the business requirements of Cloud users hence there is no need to define specific benchmarks for any QoS parameter and same should be left to mutually decide between cloud user and cloud provider within the SLA. The adoption of standards for SLAs in cloud computing service as recommended by the Cloud Innovation Council of India may be mandated for ensuring effective monitoring of the performance of defined QoS parameters.

Question 8: What provisions are required in order to facilitate billing and metering re-verification by the client of Cloud services? In case of any dispute, how is it proposed to be addressed/ resolved?

Response:
Similar to QoS performance, the billing and metering provisions are also governed by SLAs between the cloud user and cloud provider.

8.1 Billing/metering re-verification

Different service providers provide billing of their services on different basis, such as data amount, computing usage, number of users, corporate required data etc. It should be noted that the measurement methodology is often standardized by the service providers, hence, is non-negotiable. As such, billing and metering re-verification facilitation differs depending on which modal of the services has been adopted, some of which include:

a. Assessment by an independent third party
b. Request for an insight ódashboardôthat allows users to monitor usage
c. Request that the provider be subject to independent auditing assessment on billing methods (such as SOC reports)
d. Monitor and track usages through tracking tools available on the market. ó

Provisions that permit or mandate for any/a combination of the steps mentioned above will thus allow for billing re-verification.

8.2 Proposed dispute resolution mechanism

Many cloud service providers value trust from their users in respect to the use of services. As such, establishing a respectful and trusting relationship with the service providers plays an important role in dispute resolution.

Our view on the appropriate dispute resolution mechanism for billing and metering has been explained in our response to the next Question (Question 9).

Question 9: What mechanism should be in place for handling customer complaints and grievances in Cloud services? Please comment with justification.

Response:

To propose regulation for resolving complaints specifically for cloud services involve issues of applicable law, jurisdiction and access to justice. For reasons proposed in our response to Question 10, we do not support stringent, specific regulatory mechanism specifically targeting cloud services. In our view, there are other mechanisms in place, leveraging other technology neutral legislative framework focusing on consumer rights (such as right to goods and services and right to privacy), that can be utilized to resolve customer complaints in cloud services.

9.1 Leveraging other regulatory regime and authorities

Depending on the type of complaints and grievances, different regulatory and practical mechanisms can be utilised. For example, where the complaint relates to billing, the recourse can be found in consumer centric regulations, and managed by a consumer watchdog/ regulator. Where the complaint relates to privacy or security issues, recourse can be found in privacy or security orientated regulation (*our view on such legislative framework can be found in our response in Question 10 and 16*), it can then be managed by the relevant privacy or security regulator.

The question of jurisdiction, monitoring and enforcement over such providers involved the issue of effective jurisdiction. For example, how can a complaint or dispute be resolved where the service provider is based overseas? Our response to Question 14, has explained in detail, various ways in which effective jurisdiction can be established.

9.2 Alternative dispute resolution

Alternative dispute resolution mechanism, such as arbitration and mediation can also be negotiated to be included in the contracts, provided that end users have been empowered with sufficient bargaining power through legislative or contractual means.

Within the European Union, its Digital Market Agenda of ó*Unleashing the Potential of Cloud Computing in EU*ô states its aim in regulating complaints via construction of modal contractual clauses to include ófair mechanism to be utilized in the event of conflict between the users and the providersô

It is also worth noting that other initiatives commissioned by the EU include the proposal of introducing an online dispute resolution solution as possible means to resolve conflicts. The effectiveness of such utilization remains to be seen, as the proposed mechanism will similarly introduces the issue of effective mechanism and applicable law.

Question 10: Enumerate in detail with justification, the provisions that need to be put in place to ensure that the cloud services being offered are secure.

Response:

Whilst security of data has been commonly outlined as a primary issue of concern for utilizing cloud services, such utilization could in fact lead to opportunities to strengthened IT security. However, there are still apparent benefits to formal regulation on ensuring the cloud services being offered are secure, provided that such regulation is not overly prescriptive.

The consultation paper has mentioned that as predicted by Gartner that by 2020, 95 percent of cloud security failures will be due to fault at the customerôs end. The paper has further indicated that technology will be strong and secure and the only way data can be compromised is due to lack of understanding at the user side. This clearly denotes that in future, technology and IT related security processes are going to be further strengthened with the march of technology advancements hence no regulation is required in this area rather focus should be towards educating end customers/ cloud users to safeguard data at their end for ensuring end to end security of the data.

10.1 Opportunities to improve IT security

Through reinvesting the savings to the IT budget brought by the transition to cloud computing, there are opportunities for organizations to re-focus the budget to internal information security. Further, the value of the trust relationship between cloud providers and users would drive investment into protecting the data of the customers from data breaches to prevent reputational and financial damages. The engagement of subject matter experts, including information security experts by the providers may also bring forth better infrastructure, platform and service management.

10.2 Regulation on the security of cloud services

In our view, such regulation can be achieved through a principle based, technology neutral and hence future proof regulatory framework**.** Commonly, the legislative process is often a lengthy one, and may take months or even years to be passed. Technology moves very quickly, and any attempt to regulate technology services with specificity through regulation or legislation would lose relevance by the time they are passed.

10.3 Technology – neutral legislative framework

In order to remain relevant to changes to technology, regulation on the security of cloud services can be achieved through an overarching technology neutral privacy legislative framework which imposes security obligations on data controllers and processers, which will include intermediary entities such as cloud services. This can then be complemented by voluntary code of practices, guidelines, industrial standards, and modal contractual clauses.

10.4 Standards and Code of Conduct

The voluntary code of conduct and standards can also be put in place to provide guidance on the expected security conduct. New Zealand for instance, saw the development of a code of conduct for cloud services by the industry following an industry wide consultation. The code created a framework of voluntary self-regulated disclosures and minimum standards for those offering cloud-based services in New Zealand.

Further, there are existing international security standards that can be leveraged and utilized to ensure security of the service. This includes:

a. ISO/IEC 27001 ï Information Security Standards
b. ISO/IEC 27017 ï Code of practice for information security controls based on ISO/IEC 27002 for cloud services
c. ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Organizations can seek to be certified to be compliant with any of the ISO standards[8] by independent assessors.

It should be born in mind that such requirement should be voluntary. Cost of compliance to be certified in accordance to these standards are high, and a regulatory requirement to be certified may result in driving out smaller cloud service providers, hence the market being monopolized by large cloud service providers. The potential adverse impact of over-regulation of the industry can further lead to increased barrier of entries, deterrent to foreign investment and increased cost in the provision of services. This is further elaborated in Question 16 on the proposed scope of law on cloud computing.

Question 11: What are the termination or exit provisions that need to be defined for ensuring security of data or information over cloud?

Response:

[8] ISO Standards are developed by International Organisation for Standardisation.

As discussed above in response to Question 5, data subjects can be legislatively empowered with right to ownership of their data, which should include right to transfer and deletion of data, and the requirement to seek user consent when transferring or assigning usersôdata. This will in turn cover the scenarios outlined in section 4.7(a) of the Consultation Paper:

a. Provide users with the right to transfer and delete data when they so desired
b. Ensure that usersôconsent is required to transfer data when acquisition of the relevant cloud provider by another provider occurs.

In order to ensure that the data is properly deleted and no data is withheld, the regulation can be complemented with guidelines that specify acceptable data deletion and disposal methodology.

The issue concerning the effective jurisdiction over the cloud providers (in the event that such providers are not based in India) for enforcement of such regulation is discussed in response to Question 14.

Question 12: What security provisions are needed for live migration to cloud and for migration from one cloud service provider to another?

Response:

Live migration to cloud and migration from one service provider to other may raise many security concerns, including security, access and storage of the data. Detailed solutions for secured live migration to cloud and for migration from one cloud provider to another could not be provided in this instance as the solutions would differ vastly on a case by case basis. Such variables that may influence the necessary security provisions include type of legacy system, cloud delivery and deployment modal, amount of data being migrated, and the existing hardware or infrastructure. In addition, in some instances, only some data could be migrated versus other instances where full or major part of solutions and functionality can be migrated. Challenges to resolving issues concerning data portability and interoperability are discussed above in our response to Question 6.

Further, security issues can also arise at different level of the ôstackôincluding infrastructure and application security. Some of the means in which security of data could be protected is through:

a. End-to-end encryption (both in respect of transport and data)
b. Integrity check (communication protocol and data level)
c. Non-repudiation (case dependent).

Question 13: What should be the roles and responsibilities in terms of security of (a) Cloud Service Provider (CSP); and (b) End users?

Response:

By design, cloud service providers are responsible for the security element of the services offered. However, such responsibilities do not rest on the service providers alone.

Depending on the service delivery and deployment model, the providers and users will assume different level of responsibilities for security of the data.

For example, in the public cloud modal, data classification & accountability and Client & end-point protection are the responsibilities of the users regardless of whether it is SaaS, PaaS and IaaS. On the other hand, physical security responsibilities are the responsibilities of cloud service providers in all the modals. Further, depending on whether it is a private, public, or hybrid cloud model, users and CSPs will again assume different extent of security role and responsibilities. Security roles and responsibilities may also change depending on the usersô priorities. As such, it should be noted that:

a. regardless of the delivery model, overall security is generally a shared responsibility between users and CSP
b. an approach to drafting guidelines to empower users in understanding their security role and responsibilities, rather than a comprehensive manual.

Question 14: The law of the userôs country may restrict cross-border transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?

Response:

We acknowledge that there are challenges on enforcing regulations applicable to cloud service providers. In our view, effective jurisdiction needs to be established to enforce relevant regulations. Further, it is also our view that cross-border transfer should be regulated, and not restricted to fully harness the benefits of cloud computing.

14.1 Effective jurisdiction

Whilst regulations can be imposed on service providers, challenges may be faced to effectively enforce such regulations in instances where the service providers are located overseas. This can be overcome by requiring connection within the Indian jurisdiction, such as incorporation or assets. Where there is an accountable entity connected with the service providers within the India, enforcement actions can thus be taken against the entity in the event that a violation takes place.

The General Data Protection Regulation (GDPR) extends its application to data controllers (such as telecommunication providers, banking services) who are not in the EU in certain circumstances[9], thus in effect asserting extra-territorial application to overseas jurisdiction. However, how this will be practically enforced in effect has not been disclosed.

14.2 Disclosure guidelines

It is not known based on the Consultation Paper of whether the disclosure guideline referred to in this question is one to be provided by the service provider or one to be prescribed by the Government of India.

[9] See Article 3 of the GDPR, which include circumstances where the data controller or processor has an establishment within the EU, or where it offers goods and services to data subjects in the EU, or monitors their behavior.

A requirement to request a disclosure guideline for all cloud service providers would be challenging to achieve. The technicalities, time, cost and labour involved in determining where the data is stored, where the data is being transferred to, which entity has processed/held the data would result in the task being almost impossible to comply with, depending on the details required in the disclosure statement.

Disclosure guidelines that will be prescribed and issued by the Central Government on the other hand, will be welcomed to provide clear guidance on the restriction.

14.3 Cross border data transfer

It is also our view that in order to effectively utilize the benefits of cloud computing, that there should not be a blanket restriction on cross border data transfer. Cross border data transfer should in turn be regulated not restricted.

In reality, a blanket restriction on cross border data transfer across all citizens is no longer achievable today. Many online communication providers, including social networking and VoIP providers as well as a wide range of application service providers are already providing services to Indian citizens where data is processed, stored and transferred cross border. Google search engines also collect data from users each time a search is conducted.

In addition, the benefits of cloud services include the ability to remotely access the services anywhere in the world in real time, and lowered barriers of entries for local citizens to offer goods and services to a global market. A restriction on cross border data transfer will not only hinder the full exploitation of the benefits of cloud services, but also create a higher barrier of entries for local Indian businesses to enter into the international market. In the technology environment where many organisations in other jurisdictions are able to leverage the benefit of cross border data transfer to develop innovative, agile and up to date products that better suit the consumersô needs, local businesses would in turn lose out on such opportunities. End users will also be ultimately impacted, as they miss out on the opportunity for improved customer experience, improved Quality of service and innovative product offerings.

Further, the resource pooling model of cloud services means that data centers that are processing and hosting the data may be located in different locations. Forced localization of data centres in turn bring up other challenges, which is discussed in our response to Q 16.

14.4 Regulating cross border data transfer

Some of the concerns about cross border data transfer relate to national security and data ownership issues. The latter has been discussed in Question 5, 10 and 14 above. In regards to national security, this can also be mitigated through:

a. Formulating a list of countries that provide adequate protection of personal data and restricting personal data transfer only to countries on the list
b. Enforcing use of modal contractual clauses to regulate transfer of data (as it had been done in the EU)

c. Enforcing approved binding corporate rules where transfer is conducted within the same group of entities which are located in different jurisdictions
d. Achieving mutual understanding with the relevant regulators within the foreign jurisdiction on the facilitation of cross border transfer (such as the US-EU Privacy Shield that is currently being developed).
e. The APECôs[10] Cross Border Privacy Framework[11] can also be looked into as an international cooperation initiative with an aim to facilitate (as opposed to restrict) flow of data across borders and at the same time ensure consistent privacy standards.

These are the regulation that the European Union has adopted to regulate cross border data transfer. Similarly, the Government of India may publish the list of countries where cross border data can be hosted.

In addition, we also acknowledge that all the regulations discussed so far only applies to personal data, and do not cover all data. There are several ways in which protection measures could be imposed on other sensitive, non-personal data such as:

a. Use of a hybrid or private cloud for modal to store government/national security data
b. Further restrictions imposed on the transfer of data deemed sensitive by the Central Government.

Question 15: What polices, systems and processes are required to be defined for information governance framework in Cloud, from lawful interception point of view and particularly if it is hosted in a different country?

Response:
The Telenor India response to Question no. 15 and 17 should be looked at as a whole, since they both consider governmentôs lawful access to data either in a intercept (real time or near real time) context, historical communication data (meta data) or lawful access to stored data.

It is our view that instead of defining information governance framework in Cloud, which in our opinion, is difficult to achieve (due to issues such as restricting innovation and enforcement and enforcement difficulties), emphasis should be given on a clear definition of relevant policies and processes concerning lawful interception.

15.1 Local Interception

Where local interception is intended to be carried out, clear policies and processes should be set out to uphold the rule of law and ensure protection of the citizenôs privacy. As indicated by the aftermath of the revelation by Edward Snowden, a lack of transparency over government surveillance affects the reputation of the state, its relationship with other nation states as well as the citizensôtrust.

Further, it is also evident that there is an increased level of awareness over right to privacy and government surveillance. Therefore, a future proof legislative framework over lawful

[10] Asia Pacific Economic Commerce - a forum of economies recognizing importance of protecting privacy and maintaining information flows among economies in Asia Pacific region and among their trading partners.
[11] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

interception should set out appropriate grounds of interception, the relevant policies and processes, in addition to regulating the use, disclosure and access to the intercepted data.

In many jurisdictions, regulation over lawful interception is commonly set out in a separate legislation, which can be broadly interpreted to cover a range of telecommunications data, including data used, held and processed within the cloud ecosystem.

15.2 Foreign Interception

Where local interception concerns issue of foreign jurisdiction, the issue of sovereignty of different nation states comes into question. Therefore, it is thus a matter to be weighed by the Central Government on carrying out lawful interception where the services are hosted in a different country. Some jurisdictions, such as Denmark, regulate and restrict its interception activities within its local jurisdiction.

As we go forward with more complex technologies, international standards and industry standards for Lawful Intercept should be followed.

Question 16: What shall be the scope of cloud computing services in law? What is your view on providing license or registration to Cloud service providers so as to subject them to the obligations there under? Please comment with justification

Response:

Whilst we support that local regulations should evolve to ensure sufficient coverage of cloud computing, we do not support specific and stringent regulation of cloud services.

16.1 Technology neutral, future-proof legislative framework

As discussed above in our response to Question no.10, legislations and regulations are time consuming and hence will not be able to regulate the fast changing technology industry. Instead, emphasis should be given to enacting an overarching technology neutral, future-proof legislative framework. Such framework should cover:

a. Data ownership
b. Data transfer
c. Security
d. Right to access, transfer, use, and deletion of data
e. Enforcement mechanism
f. Effective jurisdiction
g. Cross border data transfer.

All of these grounds have been elaborated above in our responses to Question 5, 10, 11, and 14. A framework covering these grounds will thus formulate a solution to the challenges posted in these questions.

Such framework could be achieved through embedment to the proposed Right to Privacy Bill, or through leveraging current legislations, such as amendments to the Information Technology Act of 2000.

16.2 Localization of data centres

Section 5.25 (e) of the Consultation Paper considers the alternative of mandating the cloud service providers to host the data centres in India. It is our view that emphasis should not be placed on physical locations of the data centres, but choice of locations and overall data security (such as access) should be left to the cloud service provider.

Challenges to localizing all data centres

Often, security (including national security) and control of data are quoted as argument to localize data centres. However, there are infrastructure challenges to enacting data centres within the India. These are further outlined in our response to Question no. 20. These challenges have also been acknowledged in Section 6A of the Consultation Paper.

In addition, a requirement to establish local data centres may result in minimally-resourced facilities or operations, mediocre technologies and less skilled personnel. Instead, centralized investment in several data and IT security measures can bring higher protection than local efforts can offer. The reason behind this is that both adequate human and financial resources are allocated and the standards comply with the highest requirements of the countries served.

Backup of data within geographically diverse areas also present the advantages of spreading the risk, in the event that an unexpected event such as natural disaster occurs within a particular region. Localisation of data centres is also not cost effective, eliminating a substantial advantage of adopting the cloud service modal.

A requirement to hosting only in data centres in India will also serve as a deterrent for cloud service providers to enter the market, discussed further in below section ñ*Providing licences or registrations to cloud providers*ò

Overcoming security challenges

Instead of localization of data centres, there are steps that can be taken to mitigate security risks. These include:

a. Contractual and legislative regulations establishing effective jurisdiction and regulating the security, use, and transfer of data
b. Effective monitoring and enforcement mechanisms including certification or auditing mechanism to ensure compliance.
c. Consent requirements from data subjects over the use and transfer of their data

16.3 Data Protection Standard

The challenges in determining whether the cloud provider is meeting data protection standards could be overcome by the imposition of security obligations through the same framework (as discussed above and in our response to Question 10).

16.4 Providing licences or registrations to cloud providers

The regulatory modal of providing licenses or registrations to cloud service providers, to a certain extent, has been adopted in China and Russia. However, it is our view that such regime brings more disadvantages than advantages.

Complex and difficult requirements to enter the market, including the need to obtain registration could result in:

a. Providers encountering regulatory barriers and increased administrative, technical and operational costs, thus preventing entries for SMEs
b. Increased compliance costs, which may be passed on to the end consumers
c. The market as a result may be dominated by certain established providers, creating tension of reduced competition to the detriment of the users
d. Reduced foreign direct investment opportunities
e. Issues arise on quality of services offered through the local provider.

A stringent regulatory modal will also stifle innovation, essentially killing the advantages that could be offered through cloud computing.

Question 17: What should be the protocol for cloud service providers to submit to the territorial jurisdiction of India for the purpose of lawful access of information? What should be the effective guidelines for and actions against those CSPs that are identified to be in possession of information related to the commission of a breach of National security of India?

Response:

Lawful access to data held by cloud service providers is currently a contentious field, and differences should be drawn between data held within and outside of the jurisdiction of the Republic of India.

17.1 Data held by CSPs within jurisdiction

Where the lawful access relates to Indian data subjects held by CSPs that are located within the jurisdiction, please see our response to Question 15.1 above.

17.2 Data held by CSPs outside of jurisdiction

Where data is held outside of the jurisdiction, this relates to international sovereignty and jurisdictional issues. The challenges of determining whether access should be granted are currently being contended in the case of Microsoft Corporation Vs United States of America[12].

[12] In this case, Microsoft received a warrant issued by a District Court to produce all emails and private information associated with a certain account hosted by Microsoft. The account's emails were stored on a server located in Dublin, Ireland. Microsoft

There are several mechanisms in which such access can be facilitated:

a. Restrict data transfer only to states where human rights and privacy of data is known to be respected without excessive government surveillance
b. Achieve mutual of understanding or undertaking with foreign jurisdictions to encourage mutual assistance in law enforcement
c. Impose encryption requirements to protect sensitive data against data center seizures.

Question 18: What are the steps that can be taken by the government for:
(a) promoting cloud computing in e-governance projects.
(b) promoting establishment of data centres in India.
(c) encouraging business and private organizations utilize cloud services
(d) to boost Digital India and Smart Cities incentive using cloud

Response to 18 (a), (c) & (d):

Benefits of cloud computing can clearly be seen and has been elaborated in our response to Question no. 1 and 2. In order to promote the adoption of cloud computing by state governments, businesses and private organisations, in addition to the current cloud strategy and initiatives adopted by the Central Government, further steps that can be taken by the government include:

a. Introducing privacy and data protection legislative framework to protect the interest and rights of the citizens, thus building trust in utilizing cloud services
b. Publishing model contractual clauses, guidelines, code of conducts and policies that assist in the engagement and use of cloud services
c. Establish authorities or working parties that can provide guidance and authorities on relevant matters.

Response to 18(b):

Some of the ways to promote establishment of data centres in India can include:

a. Regulations that are easy to navigate and do not erect high barrier of entries (as discussed above in our response to Question no.16)
b. Clear and transparent privacy and data protection rules that do not create uncertainties in the operation of the data centres
c. Building confidence with potential providers through permissive ruling.

Question 19: Should there be a dedicated cloud for government applications? To what extent should it support a multi-tenant environment and what should be the rules regulating such an environment?

Response:

provided account information kept on its U.S. servers but refused to turn the other emails that were stored in the Dublin server over, arguing that a U.S. judge has no authority to issue a warrant for information stored abroad. The case is currently pending appeal before the United States Court of Appeals for the Second Circuit. Note that the Irish Government has filed an amicus brief in favor of Microsoft's position with the Court.

There are pros and cons to using different modal of cloud deployment modal.

19.1 Different cloud deployment model

Generally, using a public cloud service and infrastructure provides the advantage of minimal system management costs and more flexibility in terms of ad-hoc capacity increases. On the other hand, by retaining all data in-house, a private cloud establishment is suitable for applications necessitating strict security or regulatory compliance, which in turn, result in a much higher cost and reduced agility ï benefits that are brought by the adoption of cloud services.

Although security d cost is commonly seen as a trade-off, in reality, the cost benefit analysis of a private vs public cloud model is not as clear as it may sound. Often, reduced cost in spending on private cloud could be used to strengthen the security of the in house IT system. Further, retaining private cloud means that more time will be spent on management of the infrastructure and hardware, instead of focusing on security. Further, managing a private cloud means that all security responsibilities are placed in house, thus omitting the opportunity to leverage external subject matter experts.

Dealing with the trade-off, hybrid cloud options have been set up and offered by multiple service providers. A case for using hybrid clouds could be for instance to use a private cloud with more sensitive government data, but public cloud for less sensitive, de-identified data. Common rules regarding security such as identity and access management, encryption, intrusion detection etc can be negotiated and monitored with the cloud service providers to regulate a hybrid cloud environment, thus achieving a win-win solution of security and cost.

19.2 Multi-tenant environment

It should be noted that multi-tenancy can be a common attribute across all cloud service deployment modals, and across all layers of cloud including IaaS, PaaS, and SaaS. There is no rule of thumb or one size fit all solution in determining the degree of multi-tenancy, as it varies substantially depending on the architectural design of the software layer. In order to ensure security of data, security methods such as advanced level of security monitoring and mature incident response capability can be put in place to reduce the risks brought by multi-tenancy.

Question 20: What infrastructure challenges does India face towards development and deployment of state data centres in India? What should be the protocol for information sharing between states and between state and central?

Response:

20.1 Infrastructure Challenges

As acknowledged in section 6A of the Consultation Paper, there are some apparent infrastructure challenges that India faces towards development and deployment of state data centres in India. These include power supply, bandwidth availability and road infrastructure.

It should be noted that poor infrastructure or management on the side of the hosting country may leave cloud systems vulnerable to attack.

Without upgrading the existing infrastructure, in combination with the localization of data centers, would mean that developing and deploying data centers within India will be a costly venture that can only be undertaken by large providers, thus resulting in domination and monopolization. In addition, a data centre that is not physically secured or efficiently managed would be unsafe to operate. This will further deter the utilization of cloud service providers utilizing data centers within India.

20.2 Protocol for information sharing between states and state and central

In our view, the protocols for information sharing between states and state and central should be established based on the need and purposes of the information sharing. For example, where there is a federated modal of health care services provided between state and central government, information sharing protocol should be facilitated to enable documentation and retention of all relevant health information for treatment purposes. The framework for the information sharing can thus be established from this basis.

Question 21: What tax subsidies should be proposed to incentivise the promotion of Cloud Services in India? Give your comments with justification. What are the other incentives that can be given to private sector for the creation of data centres and cloud services platforms in India?

Response:

The possible tax subsidies regime that could be utilized to promote cloud services has been outlined in Section 6D of the Consultation Paper and we support an exploration of the outlined schemes. We also agree that tax subsidies utlilised in other jurisdictions should be leveraged to modal appropriate regime to meeting the purposes specific for India.

Other incentives that can be given to private sector for the creation of data centres can cloud services platforms in India include:

a. A government initiated plan or roadmap to upgrading existing infrastructure within India to overcome the infrastructure challenges as discussed in our response to Question no. 20

b. Support the investment not through localization or strict regulation of cloud services, but clear and transparent regulatory framework complemented by guidelines and voluntary standards and code of conducts

c. Government funded subsidiaries to building data centres

d. Creation of non-profit industrial associations such as Cloud Security Alliance to provide support and guidance to the cloud service providers.

****