



**AT&T Global Network  
Services India Pvt. Ltd.**  
*Registered Office*  
13th Floor  
Mohan Dev House  
13, Tolstoy Marg  
New Delhi-110 001, India  
CIN: U72900DL2005PTC142096

Tel: 91.11.4240 8774  
91.11.4240 8775  
Fax: 91.11.4240 8774  
www.ap.att.com

**AGNSI/TRAI/CP-Cloud Computing/2016-17**  
**August 8, 2016**

**Shri A. Robert J. Ravi**  
**Advisor (QoS)**  
**Telecom Regulatory Authority of India**  
**Mahanagar Doorsanchar Bhawan,**  
**Jawahar Lal Nehru Marg, Old Minto Road,**  
**New Delhi – 110 001**

**Sub.: Response to TRAI Consultation Paper on Cloud Computing dated June 10, 2016**

Dear Sir,

AT&T Global Network Services India Private Limited (AGNSI) is pleased to submit its response to TRAI consultation paper dated June 10, 2016 on Cloud Computing.

We trust that our submission will merit the kind consideration of the Hon'ble Authority.

Thanking you,

Respectfully submitted,  
for **AT&T Global Network Services India Private Limited**

**Naveen Tandon**  
**Authorised Signatory**

Encl.: As above



## AT&T Comments on TRAI Consultation on Cloud Computing released June 10, 2016

### **Introduction**

AT&T welcomes the opportunity to provide input to the Telecom Regulatory Authority of India's (TRAI) consultation paper on cloud computing. AT&T Global Network Services India Private Limited ("AT&T India"), an affiliate of AT&T Inc., respectfully submits these comments on the Consultation Paper on Cloud Computing, dated June 10, 2016 ("Consultation Paper"). AT&T India is licensed to provide National Long Distance (NLD), International Long Distance (ILD), Audio Conferencing and Internet Service Provider (ISP) services in India.

AT&T India is affiliated with AT&T, Inc., an integrated communications company which, through its affiliates, is operating globally to provide mobile, video and data solutions. With operations throughout the U.S. and in over 60 other countries, AT&T has extensive experience as an incumbent and a new entrant, as a fixed line operator and a wireless operator in the dynamic areas of converged technologies and services. AT&T offers enterprise services which combine mobile broadband capabilities, a huge IP backbone, industry-leading Virtual Private Network (VPN) capabilities and data centers to deliver world-class cloud computing solutions. We offer public, private, managed applications and VPN cloud services to businesses of all sizes using highly secure, scalable solutions that help businesses save costs and transform the way they work. In the Asia Pacific region, AT&T NetBond® and AT&T NetBond Essentials help multinational companies in the region enjoy the flexibility and economics of public cloud services with the security and performance of a private cloud environment. These services use regional data centers to create a highly secure path between a customer's VPN and cloud service providers.

From the perspective of a provider of global services, AT&T recognizes that the TRAI has a vital role to play in advocating for policies that reduce and avoid unnecessary burdens on global cloud applications and we encourage the TRAI to focus on regulatory policies that will allow permission less innovation that encourage all players to pursue every conceivable market opportunity, promote investment and innovation, and benefit consumers. For the reasons set forth in below in the detailed responses to the TRAI questions, AT&T presents for the TRAI's consideration the case for the TRAI to avoid encumbering cloud services solutions in India with legacy regulations that were never designed for it. Instead, regulators should let competition, innovation, and customer demand drive developments in the cloud marketplace. In the rare cases in which regulatory intervention may be appropriate, government should ensure that it is as light-touch as possible.

**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.

The opportunities and potential benefits of cloud services extend to all areas of the economy, society and government.

**Information Technology (IT) Resource Management**

Cloud computing creates a paradigm shift for business IT resources, enabling organizations to access IT and business services on-demand to maximize utilization and cost-effectiveness. As shown in figure 1, the traditional IT model required the purchase, deployment, integration, and management of all the elements that are required to deliver a business application. A cloud “as a service” model greatly simplifies application delivery.

	Traditional IT Model	Business Environment	Cloud “as a service” model	
You manage	Applications	Business Processes: How work gets done	SaaS (Software as a Service)	Managed by Cloud Vendor
	Data			
	Runtime	Applications: How work transactions	PaaS (Platform as a Service)	
	Middleware			
	O/S			
	Virtualization	Infrastructure: How work gets delivered	IaaS (Infrastructure as a service)	
	Servers			
	Storage			
	Networking			

Source: Keithrozario.com, BNP Paribas, AT&T Cloud Solutions,

<Figure 1. Traditional IT model and Cloud model comparison>

With cloud computing’s essential characteristics such as “on-demand CPU availability” (central processing unit), “pay-as-you-go pricing”, broad accessibility, resource pooling, rapid burstable elasticity and measured services, an organization can right-size resources, add more or fewer servers, storages, applications, or services, and can configure solutions to meet evolving requirements, with minimal disruption. The ability of business to scale cloud solutions with demand minimizes up front capital investment and helps avoid stranding capital investment that might be required with a premises-based equipment solution.

Cloud computing solutions also provide accelerated time-to-market delivery of new opportunities and applications, helping improve efficiency in the design, deployment and adoption of cloud solutions. For example, the scalability of cloud solutions helps minimize delays associated with hardware deployments and industry certifications. The essential cloud characteristics of speed and flexibility shine in the rapid design, roll out and adoption of new services.





### **Software as a Service**

Web hosting and email were among the first applications to be migrated to the cloud by businesses that wanted to try out the new model with workloads they considered to pose a low risk. While these applications are still among the most common cloud applications, business voice services, Unified Communications applications and contact center solutions are increasingly shifting from dependence on premises-based equipment to hosted or cloud services.

As enterprises re-distribute their applications across multiple environments, the quality and performance of networks connecting the different models becomes highly critical. Private network connectivity to cloud, such as VPNs help ensure quality of service for data as it moves among various IT environments. Furthermore, since the cloud becomes another node on the Multi-protocol Label Switching-VPN (MPLS-VPN), enterprise users can gain visibility into cloud via the application performance monitoring tools that come with MPLS solutions.

Software as a Service applications are also driving service innovation. From streaming video, to social media, to the emerging sharing economy - the market has seen how business can adopt and fully utilize cloud based design and roll-out innovative services to maximize efficiency and innovation to full potential and create global business within months, not years. These flexible and innovative business models often utilize cloud-based design and service roll-out models.

### **Remote Workers:**

The new business environment is highly mobile, and requires IT resources to be available at all times, as key stakeholders—geographically dispersed teams, partners and customers—expect to do business around the clock. This means that IT must keep IT infrastructure, applications and services running at peak efficiency, with minimal interruption or downtime.

Traditional network services, often designed to handle peak bandwidth demands, are often insufficiently elastic to address scale to fluctuating customer bandwidth demands driven by mobility and cloud-based applications. MPLS-VPNs can support on-demand bandwidth needs to enable enterprises to procure and ramp-up secure network resources in tandem with their cloud resources. Furthermore, the concept of bring-your-own-device (BYOD) is enabling these mobile users to use their own smartphones and tablets to access corporate resources; thus, making it challenging for IT managers to protect corporate data and meet compliance mandates. MPLS VPNs have inherent security mechanisms built into them to provide increased network reliability and security.

### **Internet of Things**

Even in its still-nascent stage IoT has established itself as a growth engine throughout the global economy and its importance will only continue to expand. IoT is revolutionizing entire industries by allowing Internet-connected machines to communicate directly with other Internet-connected machines, and with cloud computing platforms that analyze data coming off the connected devices, display it across user interfaces, and even provide input



and direction back to the connected devices. These machine-to-machine (M2M) communications and the associated analytics platforms, all constituent parts of the IoT, have already demonstrated the potential to greatly improve efficiency, productivity, and social welfare in fields as diverse as education, healthcare, transportation, energy, security and agriculture.

IoT technology is finding its way into almost every portion of our daily lives and our nation's economy: smart cities, connected cars, connected homes, remote telematics for almost anything with an engine, fleet management, cargo tracking, personal wearable devices for health and fitness and for medical uses, and drones, just to name a few. The applications and technologies are complex and diverse, and the potential for new IoT applications seems almost limitless. Like the app economy that sprouted in response to smartphones over the past decade, IoT presents immense opportunity for entrepreneurs and small businesses. With nearly ubiquitous wireless connectivity, Application Programming Interfaces (APIs), off-the-shelf radio modules and other electronic components, inventors have already been developing a host of innovative new devices, applications, and solutions that will bring new levels of efficiency and productivity to many different segments of our lives and the economy.

For customers, IoT will mean increased convenience and control of their lives and their environments. This extends to the government as a customer for IoT solutions as well. As with private businesses, cloud technologies will help improve government's insight into, and ability to deliver, services to their constituents. IoT solutions also provide the means for governments at all levels to move towards many policy objectives, such as IoT solutions that promote increased energy and water efficiency, improvements in public health, increased automotive safety, and better infrastructure management.

### **Big Data**

Business analytics involves new data processing techniques applied to large amounts of data, requiring high capacity of compute and storage resources and is gaining traction across industries, driving the need for faster, more flexible and more scalable computing and network resources. Organizations are looking to Big Data to unleash insights derived not only from their traditional data, but also from newly acquired social data, and from IT and network operational data.

To support line-of-business demands for big data workloads, IT departments are increasingly turning to the cloud. For cloud and hybrid business analytics deployments, MPLS VPNs can enable enterprises to procure large amounts of on-demand, secure bandwidth capacity, in real-time.

The combination of emerging IoT technologies and data analytics also will provide companies with unprecedented insight into their operations, and will help significantly improve their ability to serve their customers.

Social Media



Cloud computing has also altered the nature of how software is consumed through solutions such as social media. Cloud computing based applications provide on premises performance with essential cloud characteristics such as ubiquitous accessibility that allows users to use the application virtually anywhere, anytime. With cloud based social media, users can share pictures, videos, and messages globally in near real time.

### **E-Commerce**

E-commerce is another successful example of cloud computing adoption with its ability to accommodate major challenges like traffic surge, mobile commerce, nimble market opportunity response, and increasing user engagement. E-commerce has grown from an alternative to brick and mortar retailers, to incubating the rapidly evolving sharing economy for rides, lodging, and even household tasks.

**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?**

While business of all size benefit from the efficiencies of cloud services, the most impactful dimension of cloud services in cost reduction is actually the benefit to small businesses, where cloud services can spare these businesses the upfront cost of building an IT infrastructure and enable them to use standard applications off the cloud.

**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?**

Several factors influence business enterprise decisions, including: the preferred solution type, capital and expense budgets and the degree of in-house technical expertise. As with any enterprise grade service, security, resilience, scale, flexibility and cost are also important factors.

**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?**

**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?**

**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 to Questions 4 – 6**

The economics of the cloud ecosystem make the frictionless deployment of cloud services across global borders a business imperative. Industry players have risen to the challenges presented by the necessity for seamless international deployment of cloud technology

through a process of voluntary negotiation and innovation.<sup>1</sup> The TRAI's policy framework should prioritize support for such efforts. Thus, where there are industry best practices or voluntary frameworks already in place, the government should respect and support them. Where new standards or policies are necessary to address evolving issues, rather than moving immediately to prescriptively regulate, government can encourage—and, in some cases convene—multi-stakeholder initiatives as the first step in addressing issues associated with newly emerging cloud applications or technologies. But the policymakers must resist the temptation to reactively prescribe a “solution” for these issues that risks artificially skewing the development of the market or technology development.

In the rare cases in which regulatory intervention may be appropriate, government should ensure that it is as light-touch as possible. Policymakers also must ensure that any regulation does not inappropriately tilt the cloud services playing field. Thus, particular care must be taken to develop competitively- and technologically-neutral policies that are intended to address concerns pertaining to the cloud services solutions or a vertical within the cloud; any such regulations must be competitively- and technologically-neutral. They must also avoid singling out individual companies or business models for disparate treatment, whether favorable or unfavorable. Just as importantly, policymakers must guard against both duplication and inconsistent application by multiple, overlapping agencies with different areas of jurisdiction.

Finally, the TRAI should promote the development of standards and operating frameworks for the effective global deployment of cloud solutions. TRAI cloud policies must keep in mind the vital importance of cross-border data flows, and should not restrict the legitimate movement of data across national borders.

Indeed, the TRAI working with private industry and other stakeholders, can promote the deployment of cloud services; however, these should be industry led efforts, not mandated by government / regulators; as the development of cloud services has shown to date has shown, industry will be best positioned to create a uniform international, interoperable framework.

**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.**

The TRAI also should avoid any mandated service quality levels for cloud services as such mandates could limit the development and usage in India of innovative cloud services,

---

<sup>1</sup> There are numerous examples of successful industry-led or multi-stakeholder efforts to confront policy issues affecting the IoT in the United States. In the case of cybersecurity, the [NIST Framework](#) was developed with input from government and private industry stakeholders, resulting in a vehicle that effectively addresses the cybersecurity posture of critical infrastructure and other entities. Other notable examples are the [FTC privacy framework for IoT](#), NTIA's [UAS privacy framework](#), CTA's wearables privacy principles and the Future of Privacy Forum's [smart grid privacy principles](#). Several of these will be discussed further below.



applications and devices. These services are different services from traditional telephone services, relying on fundamentally different technology and featuring myriad different service attributes and configurations, with different capabilities and limitations and raising different policy considerations. AT&T India therefore believes that service quality is an area in which the TRAI should apply the light-handed regulation followed by many regulators with respect to cloud services and should avoid imposing strict requirements. For cloud services, examples of QOS parameters that can distinguish providers from others in the market place are: security, resiliency, scalability, flexibility, interoperability and cost. Given these myriad options, a light-handed regulatory approach to Quality of Service will best promote innovation in a competitive market.

**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?**

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

**Response to questions 8 & 9:**

AT&T is committed to providing customers an effortless customer experience. From when we design products, processes or user experiences, we strive to build “effortless” into every touch point. However, we believe matters such as customer billing and service inquiries, particularly between service providers and enterprise and multinational companies, are contractual issues that do not require intervention from regulators.

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.

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

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

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

**Response to Questions 10-13:**

At the outset, given the many variations of cloud deployment models and applications, there is no one answer that can fit all cases on this question. Migration complexity will depend on the customer environment and regulators should recognize the migration process should be governed by contractual relationship between the customer and cloud providers.



The industry is, however, already keenly focused on the security issues around cloud services. As consumer adoption of cloud applications increases, potential security vulnerabilities are likely to increase across the ecosystem as well. Cloud security, therefore, is a necessity, but a prescriptive regulatory approach is not. Businesses will have significant incentive to address security from the outset in order to succeed in the marketplace.

The general security issues raised in “Chapter 4: Security over the Cloud” are areas that various industry working groups and alliances have invested a great deal of time and study to develop guidance that will enable users and providers to ensure security in cloud arrangements. As a preliminary matter, we believe that any guidance on cloud computing, and in particular cloud security, should take the form of high level guidance that advocates usage of existing voluntary industry standards. This approach is preferable to a government mandate of specific standards given the constantly evolving nature of cyber threats and it builds upon the extensive volume of work developed by standards bodies.

Also cloud computing is designed to be distributed and may not be confined to specific geographic borders. This distributed nature combined with the fact that many cyber threats can be initiated outside of a particular country means that a focus on international and commonly accepted standards are preferable to country specific security requirements. Such an approach also provides the flexibility necessary for users and providers to enter into agreements that fit their individual needs.

Security in cloud computing, like security in many areas, does not benefit from having a “one size fits all” approach. Rather, high level guidance that remains technology neutral will encourage innovation and foster continued development within industry of security best practices that will evolve over time. For example, the Cloud Security Alliance (CSA), a collaborative industry alliance made up of more than 120 industry members has conducted extensive study resulting in its “Security Guidance for Critical Areas of Cloud Computing (Guidance)” publication. The Guidance has been updated over the years and is currently in its third iteration.<sup>2</sup>

With respect to Question 10 (provisions that need to be put in place to ensure that the cloud services being offered are secure), the CSA Guidance offers extensive, detailed recommendations and requirements to ensure the security of cloud computing. The Guidance tracks both the roles and responsibilities of cloud customers and cloud providers (Question 13) and makes recommendations to ensure a layered approach to security. The Guidance, intended to establish a stable, secure baseline for cloud operations, contains in-depth discussion of items such as physical security, application security, encryption and key management, and access management among other security considerations.

Similarly, concerning issues raised in Question 11 (termination or exit provisions for ensuring security), and 12 (security considerations for migration to another service), the CSA Guidance contemplates considering such issues at the time of contract and offers

---

<sup>2</sup> <https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/>



specific recommendations and requirements to address termination and migration. Understanding various aspects of data management, options to resume or extend with the legacy provider, as well as what security is provided by the legacy provider and who maintains access to encryption keys before migration is vital.<sup>3</sup>

The CSA guidance is one example. There are other standards related to cloud security in addition to the CSA and there have been multiple international initiatives to evaluate policy issues related to cloud computing, such as the efforts conducted by the World Economic Forum (WEF). Models like CSA provide guidance to both cloud providers and users of steps that can be taken to ensure cloud security but adopts a risk management approach that provides entities the flexibility to adopt their program to their risks as cyber threats continue.

In the United States, the National Institute of Science and Technology ("NIST") Framework (the "Framework")<sup>4</sup> is built around the concept of risk management, which we believe is the best means to address cybersecurity, particularly given the rapidly changing nature of the threats. The Framework can be a useful tool for companies to evaluate their cybersecurity risks and build a risk management plan specific to their business.

AT&T itself employs a cybersecurity risk management program that predates the Framework and that relies upon many of the same widely accepted, international security standards that map to the informative references in the Framework. We use these standards to inform our internal controls that we then apply to our network systems and to help protect customer data. Thus, the Framework serves as a complement to that program.

As AT&T recently noted in comments to NIST, the existing Framework is readily applicable to cloud services, including the IoT. Indeed, we recommended that NIST take steps to apply the Framework to a variety of issues that have come up since its publication related to IoT, including by developing use cases or examples of how the existing Framework can be used or applied in those environments. AT&T also has built on its experience with the Framework and the work we are doing with customers across many industries—as well as with our own IoT deployments—to promote better cybersecurity practices in the IoT ecosystem through a series of White Papers.<sup>5</sup>

**Question 14. The law of the user's 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?**

---

<sup>3</sup> CSA Guidance, Section II Domain 6

<sup>4</sup> <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>

<sup>5</sup> See, e.g., "The CEO's Guide to Securing the Internet of Things," available at <https://www.business.att.com/cybersecurity/>



The success of the cloud computing industry depends on the global interoperability of services and the free movement of data across borders, as well as robust protections for the privacy and security of customers' data. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it and they rightly expect that the information they entrust to cloud service providers will be highly secure and that cloud service providers will be respectful of their privacy. Establishing this trusted environment for consumers is crucial to the success of the market, separate and apart from the policy frameworks for privacy and security issues.

Governments can build trust in the cloud computing industry by ensuring that cloud service providers follow industry best practices and guidelines regarding the use and protection of personal data. The Consultation paper cites the frameworks developed by the Asia Pacific Economic Cooperation (APEC), the Organisation for Economic Co-operation and Development (OECD), and the International Conference of Data Protection and Privacy Commissioners (the Madrid Resolution of 2009), which serve as widely accepted international standards for multinational companies that collect, use, and transfer data, as well as for states when facilitating the transfer of data across borders. Rather than erecting barriers to cross-border data flows, the TRAI should ensure that cloud service providers in India adhere to principles such as these and provide strong accountability mechanisms for customers and others who wish to challenge data management practices.

Principles included in the APEC Privacy Framework include preventing harm, according to which "personal information protection should be designed to prevent the misuse of such information." According to the principle of notice, individuals should be provided with clear and easily accessible statements about "the types of persons or organizations to whom personal information might be disclosed" and "the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information." Individuals should also have notice regarding the means by which they can limit the use and disclosure of their information. The Framework also includes principles on Security Safeguards and Accountability.

These principles largely echo the principles contained in the OECD Guidelines governing the protection of privacy and trans-border flows of personal data and the 2009 Madrid Resolution of the ICDPPC. According to the former, "A Member country should refrain from restricting trans-border flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines." The Madrid Resolution establishes a similar standard. Furthermore, the Guidelines provide that "[a]ny restrictions to trans-border flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing."

**Question 15. What policies, 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?**

Governments should ensure that clear and transparent legal frameworks address the means by which law enforcement authorities obtain access to data stored by companies. Governments can also foster a successful cloud computing industry by committing to use existing Mutual Legal Assistance Treaties (MLATs) and processes when they seek access to data that is stored beyond their borders. AT&T supports government efforts to streamline MLAT processes, for example by updating MLATs to cover modes of communications associated with evolving networks and services, and to ensure that they constitute timely and efficient means of accessing data.<sup>6</sup>

**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 thereunder? Please comment with justification.**

It is important to recognize that, much as was the case with the Internet's commercial development, the developments in cloud technologies and the global spread of cloud business largely have been achieved in the absence of, not because of, government oversight and intervention. The innovation that has fueled the explosive growth in cloud computing technologies to date has been the result of private sector investment, in a climate of slight, if any, regulatory oversight.

Accordingly, it is vital for the TRAI to set a national policy framework that will support the continued, aggressive investment in the next-generation network infrastructure necessary to power the cloud computing applications and services. Over-regulation of communications networks will slow the deployment of the ubiquitous, next-generation networks over which the emerging cloud services - from software as a service Applications, to hosted VoIP applications, to contact centers, to the Internet of Things - will ride as it develops over the coming years. For years now, AT&T has made significant global investment with an eye to deploying the smart, secure, robust, software-defined network that will serve as a foundation for broad-based, economic growth. We encourage the TRAI to adopt policies with respect to the cloud computing that will help to support the continuation of this network investment more generally.

Beyond these important issues of infrastructure deployment the policy landscape is growing more complex in other ways. As cloud solutions gain adoption across a greater range of market and industry segments, and at greater scale, many stakeholders in the cloud ecosystem are finding themselves engaged with a broad array of agencies with varied roles, levels of experience, expertise, and confusing and sometimes conflicting regulatory and enforcement authority regarding cloud services. This situation is mirrored both at the

---

<sup>6</sup> See, e.g., International Chamber of Commerce, *Policy Statement: Using Mutual Legal Assistance Treaties to Improve Cross-Border Lawful Intercept Procedures*, Document 373/512 (2012), available at: <http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2012/mlat/>



national and international level. This creates uncertainty about the regulatory authority's approaches to the issues and about the cloud business opportunities in these sectors.

Given the breadth of cloud services, and their impact across virtually every sector of the economy, the assortment of agencies implicated by the cloud is not surprising. Nevertheless, the great potential for regulatory confusion through duplicative and inconsistent rules and enforcement—and, in turn, for detrimentally affecting innovation and investment in cloud technologies—is a significant cause for concern for industry stakeholders.

The potential for negatively affecting private sector investment in the networks and communications technologies that are essential to the cloud marketplace must be at the forefront of TRAI policies. The TRAI should seek to foster a coordinated framework for that minimizes regulatory burdens, provides policy clarity and certainty, creates a climate that maximizes this enabling network infrastructure investment, and recognizes the global nature of the cloud technology.

**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?**

AT&T India considers that requirements for compliance with interception and monitoring requirements should further the dual objectives of encouraging new market entrants and competition, and at the same time further the important national security and law enforcement requirements of the Indian authorities. Government authorities should ensure that clear and transparent legal frameworks address the means by which law enforcement authorities obtain access to data stored by companies. They should also commit to using existing MLAT processes in order to obtain data that is stored beyond their borders.

**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.**

Government can take many steps beyond those of regulator or enforcer to encourage business investment and boost Digital India incentives. In particular, the Government acts as an Influencer, as a Funder/Facilitator, and as a Customer. Each of these roles comes into play in establishing a sound and comprehensive policy framework for the cloud, as policymakers at all levels of the country's governments can also accelerate the deployment and adoption of cloud solutions.

### **Government Actions as an Influencer.**

Government can constructively serve in a helpful capacity as a convener of multi-stakeholder processes addressing specific cloud issues or concerns. For the right issues and with the right participants, there are likely to be opportunities for similarly productive endeavors in the future. Similarly, many government organizations produce reports on cloud related topics. The lens through which each of these agencies views and discusses the cloud will influence subsequent stakeholder thinking about the cloud, whether internal to the government, in the public, or among industry players. Here again, the TRAI can help establish a common starting point for these kinds of reports and similar actions, to aid in achieving a coordinated and coherent view of cloud services across the government.

### **Government Actions as a Funder/Facilitator**

Governments are already directly and indirectly funding some cloud solutions deployments, in India and around the world. For example, the United States Department of Transportation, for example, is directly promoting the deployment of smart cities technologies through the \$40 million it will award to the winning city of its Smart Cities Challenge.<sup>7</sup> It may also indirectly fund transportation management IoT solutions through a variety of programs authorized by the recently enacted FAST Act,<sup>8</sup> for which Congress appropriated \$337 million over Fiscal Years 16-20. As those grants will be made to state and local governments and other organizations, the program structure and grant requirements that the U.S. Department of Transportation establishes as the funder will significantly affect how any IoT solutions are brought forth from this and other programs.

The government can and should continue to fund pilot programs and challenge grants, as with the example from the United States. These kinds of programs can provide a helpful kick start towards development and adoption, and produce valuable learnings for the private sector and governments alike. Similarly, government agencies should coordinate and streamline the processes for applying and obtaining approval for establishing supporting facilities, including data centers and wireless infrastructure.

Governments can further facilitate a more rapid deployment of IoT, particularly in the areas of smart cities and transportation, by encouraging the incorporation of IoT and networking technologies into public works and infrastructure projects, and by enabling access to public data through APIs and IoT platforms.

### **Government Actions as a Customer**

The promise of cloud services for enhancing the efficient delivery of government services is profound. In government's role as a significant customer for cloud services, government adoption of the cloud services can be improved through continued efforts to

---

<sup>7</sup> See <https://www.transportation.gov/smartcity>.

<sup>8</sup> For example, section 6004 of the FAST Act directs the Secretary of Transportation to "establish an advanced transportation and congestion management technologies deployment initiative to provide grants to eligible entities to develop model deployment sites for large scale installation and operation of advanced transportation technologies to improve safety, efficiency, system performance, and infrastructure return on investment."



simplify and streamline government purchasing, and coordinating between policy-making and acquisitions components of governments. Doing so will help governments (and thus taxpayers) reap the same sorts of transformative benefits in business processes and efficiency that so many sectors of industry are seeing from cloud adoption.

Again, using IoT as an example, IoT fleet and asset management technologies can produce operational savings for many government agencies that operate large vehicular fleets or that engage in frequent shipments of goods. Similarly, IoT solutions, from smart thermostats and smart grid solutions to security services enabled by IoT capabilities, are beneficial to any government entity that manages facilities. In these and many other areas of cloud services, the government is not yet well equipped to purchase cloud solutions for itself. Increasing the flexibility and adaptability of its acquisition processes to incorporate the purchase of cloud services will help foster more rapid adoption across the economy.

An example of steps the government can take can be found with the US Federal Risk and Authorization Management Program (FedRAMP) program. Recognizing the benefits of clouds solutions, the program was established to mitigate security concerns to promote cloud computing within government agencies. The institution of the US Federal Risk and Authorization Management Program (FedRAMP) certifies cloud computing solution is sufficiently secure before it is deployed by any agencies. The program provides a common set of governance for all agencies allowing them to adopt cloud universally, avoiding the time, expense and integration challenges that would arise if each agency was to develop individual requirements.

**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?**

**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?**

India is a leader in the information and communications technology sector, and it is important that it continues to set an example by eliminating regulatory barriers to the free flow of data across borders. A successful cloud computing industry depends on global interoperability of services and the free movement of data across borders. We recognize the need for legal regimes that respond to evolving technology through fair, uniform procedures that strike a fair balance between privacy and law enforcement. However, these interests must be balanced against the need for cloud service providers and consumers to move data as they see fit. Numerous studies have indicated that the restriction of cross-border data flows by means of local data storage requirements and other policies has a negative impact on the ICT sector and a state's economy as a whole.<sup>9</sup>

<sup>9</sup> See, e.g., William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwachter, *Internet Fragmentation: An Overview*, World Economic Forum (January 2016), available at:

[http://www3.weforum.org/docs/WEF\\_FII\\_Internet\\_Fragmentation\\_An\\_Overview\\_2016.pdf](http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf); Business Roundtable, *Putting Data to Work: Maximizing the Value of Information in an Interconnected World* (2015); International Chamber

According to the World Bank's 2016 World Development Report,

Cross-border data flows are likely to increase with the increasing use of cloud computing, which relies on data flowing back and forth as users retrieve and update information directly on the servers. Barriers to data flows will force firms to relocate tasks and operations, change their information technology (IT) architecture, engage a different supplier, or discontinue services to customers. These barriers disrupt two of the most important business trends facilitated by the internet: the fragmentation of production into global value chains, and the creation of offshore service hubs like the business-processing operations in India or the Philippines.<sup>10</sup>

Business Roundtable reports that restrictions on cross-border data flows are harmful to innovation in areas such as cloud computing, IoT, the use of Big Data analytics, business back-office consolidation, and supply-chain automation, and it indicates that the global benefits of cloud technology "cannot be achieved by an isolated cloud limiting data flows to a single country." Furthermore, restrictions on data flows frustrate the international community's goal of a free and open Internet and may not be effective means of protecting consumer privacy.<sup>11</sup>

The TRAI should avoid erecting discriminatory and protectionist barriers and consider specific provisions designed to protect the movement of data, subject to reasonable safeguards like the protection of consumer data when exported. The TRAI should likewise consider that to support the Digital Economy in India, companies should not need to build physical infrastructure and expensive data centers in every country they seek to serve, as this requirement adds unnecessary costs and burdens on providers and customers. TRAI policy likewise should take into account that if some states adopt data localisation mandates, others are likely to follow. This approach would frustrate the capacity of multinational companies to establish call centers, data storage facilities, and other operations in India. Therefore we urge the TRAI to confront these localisation barriers through specific provisions designed to promote access to networks and efficient data processing.

---

of Commerce, *Localization Barriers to Trade*, Policy Statement 103/323, available at: <http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2014/ICC-POLICY-STATEMENT-Localization-Barriers-to-Trade/>; Daniel Castro and Alan McQuinn, *Cross-Border Data Flows Enable Growth in All Industries*, The Information Technology and Innovation Foundation (2015), available at: <http://www2.itif.org/2015-cross-border-data-flows.pdf>.

<sup>10</sup> See <http://www.worldbank.org/en/publication/wdr2016> at 300.

<sup>11</sup> See, e.g., Outcome Document of the High Level Meeting of the General Assembly on the Overall Review of the Implementation of WSIS Outcomes (2015), available at: <http://workspace.unpan.org/sites/Internet/Documents/UNPAN95735.pdf>; NetMundial Principles (2015), available at: <https://www.netmundial.org/principles>; Global Commission on Internet Governance, *One Internet*, Centre for International Governance Innovation and The Royal Institute for International Affairs (2016), available at: <https://www.ourinternet.org/report>; Freedom Online Coalition, Statement on Restrictive Data Localisation Laws (Summer 2015), available at: <https://www.freedomonlinecoalition.com/wp-content/uploads/2015/09/2015-13-FOC-joint-statement-on-restrictive-data-localisation-laws-pdf1.pdf>



### Conclusion

As AT&T has discussed in these Comments, it is critical that the TRAI develop a policy framework for cloud services that can help ensure the on-going, robust network deployment necessary to support this technology into the future. The TRAI's policies must minimize regulatory burdens, and provide policy certainty that will create the climate to maximize essential infrastructure investment. The key attributes of that framework should include:

- support for the collaborative, self-regulatory initiatives among industry stakeholders that have fueled the growth of the cloud services industry and benefited small and medium enterprises to date;
- in those limited cases where regulatory action may be justified, use of a light touch, flexible, well-coordinated regime that protects innovation and facilitates rapid cloud market developments;
- clear and transparent rules governing law enforcement access to data and a commitment to follow existing mutual legal assistance procedures; and
- a policy framework for cloud services that facilitates international interoperability and the seamless global deployment of cloud services.

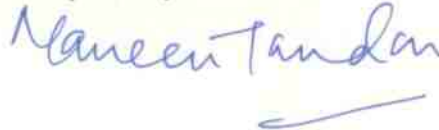
\*

\*

\*

AT&T India would be pleased to provide any additional information that would be helpful to the Authority.

Respectfully submitted,



August 8, 2016