Symantec's Response to TRAI Consultation Paper on Cloud Computing Released for Public Comments on June 10, 2016

About Symantec

Symantec Corporation is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Executive Summary

1. First and foremost, cloud computing is not a new technology per se. Rather, it is a continuously evolving business model of providing and using Information Technology (IT) products & services while combining existing technological capabilities.

2. Most though not all Information and Communication Technology (ICT) products and services are already moving to the cloud. The Authority is well aware that the various issues listed in the consultation paper with respect to the cloud computing are applicable to the Internet in general.

3. No *ex ante* regulatory intervention is warranted unless and until there is a market failure and even then, it can be demonstrated that the regulatory solution is solving such market failure.

4. All cloud services are accessed over the telecom network infrastructure services of the telecom licensees in India. While cloud services are actually beyond the scope of the telcom licensing framework, these are already adequately regulated under the Information Technology Act.

5. Considering diverse user needs and different options available, it is best to leave it to market forces to determine:

   a. What, how, when and why someone moves to the cloud and if so, the model thereof.

b. Contractual arrangements with respect to Quality of Service, Service Level Agreements, exit /migration and interoperability, Dispute Resolution & Grievance Redress.

6. Consensus-driven voluntary standards are being developed and deployed with participation of providers and users thereby obviating any need for regulatory intervention.

7. Unfettered and secure transmission, storage and processing of data are a pre-requisite for instilling trust amongst the stakeholders besides enabling resilience.

8. Concerns around security and privacy are valid. Hence, the Authority should recommend adoption of baseline security and best practices. These could include ‘security by design’, ‘privacy by design’, ‘default encryption’, ‘strong passwords’, etc.

9. Rather than mandating data localization, India should consider policies that incentivize investment in the data center infrastructure and usage of cloud computing within India. Mandatory storage and processing of data would increases costs and decrease efficiencies besides undermining growth prospects of India’s IT exports exceeding USD 100 billion. In fact, India’s It exports are predicated on the ability of cross-border free flow of data and in fact, a manifestation of cloud computing even if it is rarely perceived or referred to as such.

10. Government can and should lead in usage of cloud computing.

11. Joining Council of Europe’s Cybercrime Convention would enhance ability of India’s law enforcement agencies in countering the growing menace of cybercrime.

12. Considering the recent development specifically with respect to privacy in European Union by way of General Data Protection Regulation (GDPR), it would be desirable for India to work towards an agreement similar to the ‘Privacy Shield’ or a suitable adequacy framework that would both ensure security obligations for data transfers but would also enable unfettered and unrestricted flow across borders. This is crucial for India to sustain its leadership in global outsourcing market.

Responses to the Specific Questions Enlisted in the Consultation Paper

Business Value of Cloud Computing

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.

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?

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?

What, when, how and why to use the cloud would depend on an organization's evaluation of perceived benefits and risks with respect to their own focus, needs, budgets, technical skills, financial resources, critical functions, requisite scale, flexibility and seasonality of the operations, extant regulations and physical infrastructure. Businesses should assess what data assets and what computing processes they have, categorize them between those that can or should migrate to the cloud and those that cannot or should not.

Cloud computing also helps in several other ways. For example, an enterprise may find it much more economical to use standardized cloud services for email security at an external world-class gateway rather than having to deploy something in-house that may be limited by the skillsets as well as the scalability and speed.

In particular, a micro, small or medium enterprise (MSME) may often prefer to focus directly on its core business and rely on specialist service providers on non-core functions and cloud computing is a often a good choice for them to use in addition to basic in-house IT infrastructure.

Neither all the data nor all the processes need be in the cloud, at least not in any random or uncontrolled cloud. The same applies for the choice of the deployment model such as public, private or hybrid.

Use of Cloud by and within the Government

Question 18. What are the steps that can be taken by the government for:
(a) promoting cloud computing in e-governance projects.

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?

Indian government has already adopted the dictum of ‘Cloud. Indian government has already adopted ‘Cloud First, Mobile First’ dictum for e-governance and cloud would definitely be a great enabler in realizing the ambitious ‘Digital India’ program. In fact, online authentication using India’s national biometric ID ‘Aadhaar’ initiative is already the world’s largest such endeavor.

Central government in India has already created ‘Meghraj’ – the government’s own private cloud. Several state governments and other public sector entities are also undertaking similar endeavors. On the financial side, the government may consider suitable public subsidies (direct as in the form of money and indirect as in tax franchise for example) as acceptable under the WTO state aid rules.

There is a case to be made that some government applications are best hosted on a government private cloud (as opposed to commercial clouds available in the market). How big that cloud needs to be and what functions it needs to host is the prerogative of the respective government agencies. Multi-tenancy is a desirable feature because the bigger the resource, the higher the number of tenants, the larger would be the economies of scale.

At the same time, it is worth reflecting on where the boundaries of the government cloud should be set, and how it should be made to federate with commercial clouds, considering that commercial cloud services may be both more agile and economic compared to the government’s own cloud.

Last but not the least, the architectural design and the procurement of the government cloud should be technology-neutral and choose best options available rather than choose technologies emanating from a particular business model or philosophy or geo-location. For example, a particular technology should be used if and only if it is best of the breed and not just because it happens to be indigenous. This is particularly true of security, since the government cloud is certainly the crown jewel to defend, so it needs the best security capabilities available.

Migration & Interoperability Across Cloud Providers

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

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

Cloud service providers tend to facilitate migration and portability in creative and innovative ways without regulatory intervention, because every cloud vendor has a business interest to attract customers from their competitors and will make available tools to facilitate such migration.

The simplest form of migration could be just by export of the data by the incumbent provider to the new one. So long as the incumbent provider does not “lock in” the data by technical means that frustrate the customer’s choice for migration, portability is generally not an issue. However, just in case there is a situation that subverts free competition in the marketplace, Competition Commission of India is the appropriate forum to look into such matters.

In addition, for some SaaS services where no data is stored by the cloud service provider (e.g. Symantec’s email Security.cloud), migration is as easy as rerouting the traffic from one email gateway to another one.

Ultimately, migration path will depend on the needs of each specific case and the available options. However, when it comes to security the cloud provider should give appropriate security assurances and commits to predefined service levels that will be relevant and sufficient to safeguard the integrity, confidentiality and availability of everything, depending on the type and volume of data and processes to migrate. In doing so it should ensure appropriate organizational and technical controls during the migration process such as the use of authentication and encryption technologies.

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?

Going by the first principles, if there is no evidence of market failure, there is no need for any regulatory intervention at all.

Both open source and proprietary technologies have their respective advantages and disadvantages. Businesses and users should have total freedom of choice when it comes to open source or proprietary or any combination thereof, unfettered by any regulatory fiat.

In the long term, certain models and practices may be more prevalent than the others. However, it would be ingenious to pick and choose winners by way of regulatory intervention that could do more harm than good.

In any case, where technological standardization is considered, for the cloud of all areas, it is crucial that standardization efforts be market-led, transparent, open and inclusive, always technology-neutral, outcome oriented and globally compatible. As the works across borders by nature, any local standard would undermine its very ideal and deprive achievable economies of scale. Moreover, there is a lot of work already underway at global level and it would d be best for Indian government, businesses and experts to participate and contribute therein rather than undertaking isolated and disjointed in-country endeavors.

Data Ownership & Control

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?

The Authority must appreciate and take into account subtle yet extremely crucial distinction between the three different types of data.

Firstly, there is data created or stored by the customer into the cloud and for this, the customer should have the right to control and recover, and obtain its erasure from the cloud. This data can be further categorized into personal data usually regulated under data protection or privacy legislation; and, intellectual, proprietary or confidential data which is non-personal but of commercial value nevertheless such as intellectual property and other business information.

There could be second type of customer data as well, that is created, collated or derived by the cloud provider in the course of the customers' use of the cloud service. Ownership of such data should be with the cloud provider without any right of the customer *per se*. Of course, such data may need to be anonymized/de-identified from the respective customer, but the cloud provider should have the unalienable right to keep the data and to exploit it even after the customer has left or migrated.

For example, a cyber security company should be able to retain the data that goes into its threat intelligence because without knowledge and memory of a past threat another individual may be victimized by the same threat; The threat intelligence developed and generated through detection telemetry collected from customers' devices is the result of the endeavors and intellectual property of the service provider. In such cases, there is no need to go into the respective databases and erase every artifact captured from a particular customer even if or after that customer chooses to stop using that product or service. It would neither be feasible nor in fact is desirable to do so. In fact, erasing such data would be counter-productive from a security perspective as explained earlier.

Admittedly, the discussions have ensued in the context of even in the non-privacy space (e.g. Internet of Things) around whether, for example, geo-location data of cars should belong to the car manufacturers, to the supplier of the navigation systems in the cars or to the individuals driving the car. However, these developments are in very early stages of maturity.

Contractual Obligations, Dispute Resolution & Grievance Redressal

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? Essential versus desirable parameters and their respective benchmarks may be suggested.

Neither there can nor there should be uniform and common metrics for all cloud services, since all of them serve different purposes in different ways, using different media and based on different business models. For example, the performance indicators which will make sense in the service level agreement (SLA) of a cloud-based email security service will have nothing in common with those for a cloud-based backup service, and neither of the two will be comparable in any way to the relevant performance indicators of IaaS (Infrastructure as a Service) or PaaS (Platform as a Service).

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.

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

Since there is no universal singular business model of cloud services, it is neither realistic nor desirable to expect or even accept a common set of metrics. Metrics for service level and performance are a matter of mutual contract between the cloud provider and its customers and the normal dispute resolution mechanism should be used as and when needed. Yes, greater awareness may need to enhanced transparency, efficiency and predictability in such arrangements.

Security Considerations

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.

Security is indeed a very important consideration when it comes to cloud services. CSPs can actually play a role in not just ensuring and improving safety and security of the services they provide but also offer Security As a Service. Kindly allow us to elaborate;

- Cloud providers themselves would need to ensure that their services are safe and secure, meaning resilient, with adequate confidentiality, integrity and availability. This could be achieved notably (as in the European model) through:

  - An obligation to take technical and organizational measures to manage cyber risk to the cloud service at all times

  - An obligation to detect and report cyber incidents impacting the resilience, integrity, confidentiality or availability of the cloud infrastructure / service / platform. Where an incident only affect one or a few specific cloud users only, reporting could be confidential and to those customers only.

  - An ability to transparently demonstrate compliance to those provisions by way of non-repudiable proofs of compliance, audits, relevant certifications and other forms of cooperation with supervisory agencies.

- On the other hand, cloud providers should also be encouraged to make security as a service available to their customers in a way that can be adapted and tailored to the different needs of each. This ensures that security apart from being a legal obligation becomes also a source of revenue and a potential competitive advantage for cloud providers. This could include:

  - A requirement to ensure adequate authentication mechanisms to ensure that only authorized users of the customer can access the cloud resource (our VIP and MPKI can do that)

  - A requirement to make available to the customer metrics on the security posture and cyber risk profile of the cloud infrastructure / platform / service in real time. Metrics for the same should be defined in consultation with relevant stakeholders including but not limited to the cyber security vendors, be transparent and auditable.

  - A possibility (not necessarily a requirement but a lawful option) to provide security as a value added service as part (or on top of) the main underlying cloud service.

'Securing the Cloud for the Enterprise'[1], a Joint White Paper from Symantec and VMware delves into key elements of security at different layers, viz. Infrastructure, Information, Identity and Devices.

[1] http://eval.symantec.com/mktginfo/downloads/21187913_GA_WP_SecuringtheCloudfortheEnterprise_05%2011.pdf

'Keeping Your Private Data Secure'[2], another White Paper from Symantec describes how encryption helps achieve both security and privacy. It describes use of encryption at end-point devices (computers, mobile devices and even the 'things' being connected to the Internet); Files & Folders; the E-mail and even the web (SSL).

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

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?

The legal constraints on the user should not extend to the cloud provider and thereby binding the latter, and rightly so. The cloud provider may not know what kind of data the user is putting in the cloud, and what restrictions may apply to a particular type of data.

Though somewhat counter-intuitive, the question actually needs to be reversed.

It is the customer's responsibility to know what they can and cannot do with respect to certain type of data and hence, they must make an informed choice and decision about using the cloud for the same accordingly. For example, if a certain type of data cannot be exported out of the country on account of any regulations, the customer should choose a cloud provider who meets the requisite conditions and ensure that the same are clearly chalked out in the respective contract.

Law Enforcement Access

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?

Firstly, cloud is about achieving efficiencies through consolidation of data centers that are interconnected via resilient telecommunication links.

Notwithstanding the location for storage of data with respect to any particular user, service or use case the existing norms for lawful interception and monitoring under the extant laws within are applicable. Cross-border data communication is similar to the international telephone calls in that sense.

[2] https://www.symantec.com/content/dam/symantec/docs/white-papers/keeping-your-private-data-secure-en.pdf

However, how the rules are applied, is a prerogative of the government. These may include but are admittedly not limited to the following:

- For data hosted within the territory of India, the legislature has to decide whether or not to apply mandatory data retention, data preservation and lawful interception requirements on cloud providers, as they normally apply already to telecom licensees and ISPs.

- For example, under the current regulatory regime in Europe, only telecom licensees and ISPs are subject to lawful interception rules, and most data retention rules that exist in the various EU member states also focus on them only. The Council of Europe Convention on Cybercrime provides a list of remedies and procedural measures for cybercrime investigations that would be appropriate also in the case of cloud infrastructure located in the territory of India.
- For data hosted outside of the country, the best avenue available at the moment is to join the Council of Europe's Budapest Convention on Cybercrime that inter alia contains provisions on remote search and seizure and mutual legal assistance. The procedure there would be that India concludes specific international agreements or relies in the mechanism of the Budapest convention with third countries whereby Indian authorities are allowed to remotely search data repositories in that third country following a certain pre-established due process, on the understanding that the authorities of the third country would have similar reciprocal rights with respect to data hosted in India.

    - Since this last scenario is very theoretical and quite unlikely to be workable in the near future (even among EU member states it is still very much a utopia), the alternative for now remains to work with mutual legal assistance treaties (MLATs) agreements, which will be only as effective or ineffective as the respective governments are able and willing to negotiate, collaborate and cooperate.

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?

Providers with a physical presence in the country should be subject to the law of the country. For those without any physical presence, can appoint a representative in country who would be the contact point and control point through which national jurisdiction is exerted over the cloud provider.

As for the question of "CSPs in possession of data" related to national security breaches, the moot question worth probing is whether the CSP has – or can or should have – any knowledge of the data that the users puts in the cloud. In fact, the government may not even want a Cloud Service Provider to inspect the data of all its customers in search of sensitive data pertaining to national security.

Under European e-commerce law, cloud providers who only convey, cache or host user data are not liable for the content of such data, unless they are informed that there is something wrong with the content, in which case they must take action to have it removed. A similar system could be thought of here. However, what is important to bear in mind is that:

- The responsibility to detect information that's relevant to national security should not be delegated to the cloud provider, who has neither the authority, nor the legitimacy, nor skills, nor more importantly the need to know or determine what is relevant to national security.

- At the same time there should be some due diligence in terms of cooperating with competent authorities through due process and under the rule of law to facilitate official investigations (see question 15)

Licensing & Regulatory Framework

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 thereunder? Please comment with justification.

There can be no such thing as a "scope" for cloud computing services. Anything and everything can be or become a cloud service. Trying to define a scope in law would essentially mean chilling innovation and setting the boundaries of cloud irrespective of what technological and business model innovation may evolve. Cloud is not a technology; rather, it is a new business to deliver storage and computing services remotely through a novel approach to architectural design.

Hence, any proposal to bring in a licensing or even registration system would be a backward step considering that:

- Almost everything on the Internet (and, increasingly on mobile) is already a manifestation of 'Cloud' and if not, it would very soon be.

- All cloud services are accessed over the network infrastructure services of telecom licensees.

Conducive Policy for Attracting Investments

Question 18. What are the steps that can be taken by the government for:
(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.

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?

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?

For many services, data would have to traverse across central and state governments. For example, while a student may be provided scholarship by the state government but the identity authentication with Aadhaar would be done by the central government. Hence, it would benefit the country to deploy central and state data centers efficiently in the spirit of 'cooperative federalism'.

On the financial side, public subsidies (direct as in money and indirect as in tax franchise or land allocation, for example) must be compliant with the state aid rules under WTO.

On the legislative side:

- Creating a policy context that accepts and encourages unhindered international data flows. The underlying point is that locking or restricting Indian data within the Indian jurisdiction or applying excessive licensing or national security considerations would be counter-productive as any such barrier would be reciprocated by other countries and thereby in the long run, undermine the very value proposition of cloud and such other paradigms. Moreover, it would still not prevent Indian citizens and businesses from using cloud services readily accessible over the Internet and located in other jurisdictions.

- In particular creating a regulatory framework whereby overseas customers (including but not limited to those from places like North America and Europe) will confidently and easily choose to have their data hosted in India, for instance by achieving that India's privacy regime is recognized as "adequate" by the European Commission under the EU privacy law, and by putting in place mutual legal assistance treaty (MLAT) and other cooperation treaties with governments of key international partners (such as the bilateral cyber framework signed with the US in August 2016) so as to facilitate cooperation of law enforcement and national security agencies with respect to data in the cloud.