Cloud computing is increasingly becoming a new means of delivering and procuring IT service. Cloud adoption provides the opportunity to meet business requirements by leveraging the availability of cost effective, scalable and dynamic IT resources and the expertise of the cloud service providers. With the current worldwide IT spending of USD 3.6 trillion, a significant portion of it could be potentially spent on procurement of cloud services. Currently only around USD 131 billion is being spent globally for public cloud, as per Gartner and it is predicted that the Asia/Pacific (India & Indonesia) and Greater China & Latin America would emerge as the fastest growing markets with respect to all new public cloud spending between 2013 and 2016.

Enormous opportunities exist in the cloud that could be exploited through its adoption, but at the same time various new challenges and issues have emerged that threaten its adoption. These issues may range from the technology to legal to public policy. Many surveys have revealed that the legal and policy related issues in security and privacy are major hurdles in cloud adoption. These issues include geographic location of systems and servers, government imposed restrictions on cross border data flows for privacy protection and security, difficulties for law enforcement agencies (LEAs) in undertaking crime investigations and capturing cyber forensics, difficulties for intelligence agencies to perform surveillance and interception in the cloud, difficulties faced by government authorities in getting lawful access to data on the cloud, among others. To solve many of these issues, governments have a major role to play.

To discuss some of the above challenges and find some possible solutions, a workshop was conducted by DSCI and BSA on July 16, 2013 in New Delhi. The workshop was chaired by Dr. Kamlesh Bajaj, CEO, DSCI. The industry was represented by leading cloud service providers including TCS, Intel, Autodesk, Wipro, Symantec, CtrlS. A senior official from DeitY represented the government. A legal expert was also invited to the workshop to specifically discuss the legal challenges and applicability of Indian laws in the cloud environment.

Many issues pertaining to cloud were brainstormed in the workshop and few important ones are discussed in this note.

**Data Classification Technology**

One of the main concerns highlighted was that of arising conflicts between the global nature of cloud and Internet architecture and delivery and the local legal and regulatory requirements. A cloud service provider could have datacenters, clients, end customers and resources maintaining the services – all in different geographic locations. However, national security, cyber security, privacy and content regulation related legal and regulatory requirements may require cloud service providers to comply with local requirements, making it a daunting task for the cloud service providers. In many instances, the compliance requirements could be such that they may dilute or attempt to dilute the very benefits of the global architecture and benefits of cloud services.

It was highlighted that today there is no technology available that enables cloud service provider
to classify data based on the certain parameters esp. those that could help classify data as lawful or unlawful and help cloud service provider comply with local laws based on data segregation. In this regard, interpretation of section 79 of the IT (Amendment) Act, 2008, on intermediaries, in the cloud environment, was discussed. The safe harbor rules require intermediaries to undertake due diligence to ensure that data which is unlawful (defamatory, grossly harmful, obscene, etc) is not dealt (stored, processed, transmitted, etc) with by the intermediary and is removed when it comes to its knowledge, in order to comply with the rules. For a cloud service provider, identifying such unlawful data may be practically impossible – in many cases (e.g. storage as a service), the cloud service provider may not even be authorized to know what data is stored on its cloud (confidentiality agreement with the client).

Taking the global architecture and delivery versus local regulatory regimes discussion ahead, it was highlighted that in many instances the legal and policy direction of countries may contradict or challenge the very characteristics and properties on which the Internet was designed and is run (e.g. anonymity). The growing concerns of the governments on national security, cyber security and privacy may require changes in the global architecture of the Internet and would have significant impact on the public cloud services.

**Cloud Forensics**

With the proliferation of the cloud adoption in the B2B and B2C segments, including in various critical and sensitive areas, cloud forensics is becoming an important element. Forensics capabilities should be viewed as an enabler of cloud adoption and a driver to increase trust and confidence in the cloud. But the existing gap between the demand and supply of required set of skills and technology in cloud forensics is quite huge. In case of any crime investigation, uninformed and unskilled investigator may create unnecessary burden on the cloud service providers and also create hindrances in their regular operations. It was emphasized that the LEAs need to be trained in the cloud forensics through various programs. Government and industry need to collaborate on this front. DSCI’s Cyber Labs initiative for capacity building of LEAs in cyber-crime investigations and cyber forensics was highlighted as a good PPP example in this regard.

**Digital Certificates**

Another issue which was highlighted was the non-recognition of the root certificates authorized by the Indian Controller of Certifying Authorities (CCA) by many of the imported software products that are leveraged by the cloud service providers to deliver cloud services. This results in the loss of business opportunity for the cloud service providers with respect to serving Indian customers that use CCA’s recognized digital certificates. This non-recognition of Indian root certificates and recognition and usage of foreign digital certificates in products could also create jurisdictional issues as the latter can make it tough for LEAs to get the logs and other details from a foreign digital certifying authority. The jurisdictional problem, however, can be solved having mutual agreements between Indian and foreign certificate authorities. However, few participants refuted this issue of non-recognition of root certificates issued by Indian CCA, highlighting that the software imports do recognize such certificates. This matter requires
further investigation.

Encryption

Encryption standards are essential to strengthen the security of the data residing in the cloud. But variance in the legal and regulatory requirements vis-à-vis minimum and maximum limits on the strength of encryption standards create challenges for the cloud service providers when it comes to meeting monitoring, decryption and interception related regulatory requirements. In this regard, the 40-bit limit on encryption standard as part of the DoT’s telecom licensing conditions and section 84A (encryption policy) of the IT (Amendment) Act, 2008 were discussed.

Also, regulation of sensitive dual use technologies such as encryption was also deliberated in the context of cloud services. Technology that could be used for both civil and military purposes is termed as dual use technology. To avoid the misuse of technology, restrictions on export of such technology are imposed. Internationally an arrangement, known as Wassenaar Arrangement has been established for this purpose. Under the Wassenaar Arrangement, identified sensitive technologies are exported to member countries and export is restricted to countries listed as dangerous. It was brought to light that India is not a member country of the Wassennar Arrangement and this may create some barriers in procurement of cloud services. However, a detailed study on how the Wassennar Arrangement will relate to and impact cloud services needs be undertaken.

Export and Import Controls maintained by the US

The US restricts export of state-of-the-art technology through Export Administration Regulations (EAR). It was highlighted that export of cloud services from US to India may fall under the EAR. There is also a Trade Agreement Act (TAA) list maintained by the US which permits federal acquisition of US-made or designated country end products, or US or designated country services, and denies procurement from any other country. India does not feature in the TAA list, and this exclusion, prima facie, could impact delivery of cloud services from India to US federal agencies. However, as with Wassennar Arrangement, both EAR and TAA need to be further studied to analyze their impact on export and import of cloud services between US and India keeping in view the existing trade relationships between the two countries esp. those related to outsourcing industry.

The Cloud promises immense benefits for businesses and even governments. The global technology architecture of the Cloud and the Internet are making it possible to deliver benefits and value including elasticity, cost advantage, flexibility, user experience, among others. The geography specific regulations may sometimes contradict or challenge the cloud architecture. There is a need to build trust and collaboration between governments and the cloud industry and evolve global mechanisms to facilitate cloud adoption. The national concerns esp. those relating to national security are important, and must be respected by the industry. However, the solutions to challenges must be pragmatic, forward leaning and business friendly. Cloud is being claimed as the next growth frontier for the IT industry, and it could only be exploited to its full potential, if there is global consensus on the solutions to the issues hampering cloud adoption including those discussed in this note.