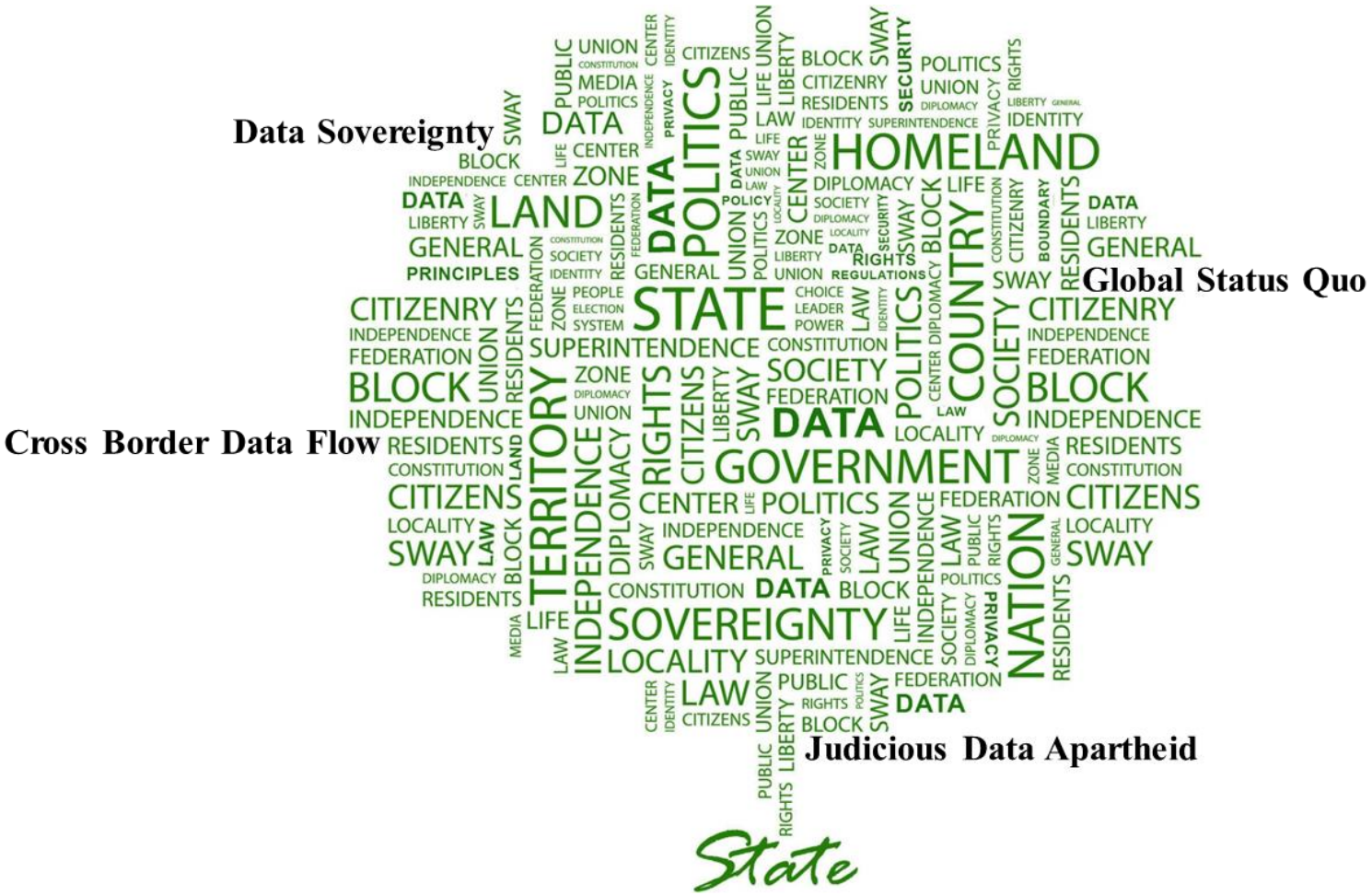
Architecting the digital future...

How Well Do We Understand…



?

01 January 2016

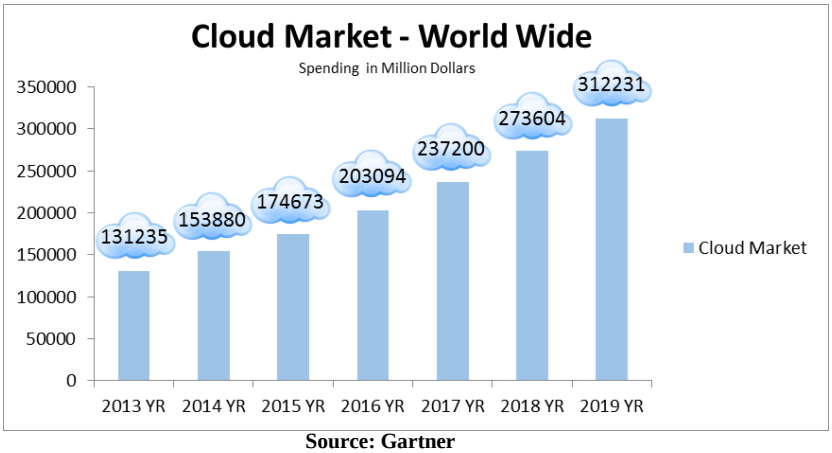
Abstract:

The renaissance that the world is witnessing in the technology space today owes to the ever growing and never ending technology needs. The enterprises are taking leaps towards serving their customers better each day in the quest to establish their relevance within customer's business ecosystem. This has resulted in technology reincarnation viz. Big Data, Hyper Cloud, IoT, Software Defined Everything and the bouquet of "As a Service" solutions. Most of these are no more options to be chosen from, but are strategic choices for any enterprise aiming to accelerate in the competitive market.

The momentum enjoyed by these services, owes to the cost optimization and the efficiency they realize.

The observation is supported by some staggering numbers thrown by industry experts and analysts like Gartner, which show an estimated increase in the cloud spend globally from USD 1,31,235million to USD 3,12,231million between 2013- 2019.

These services through their global presence and availability have eradicated the constraints of data being seamlessly made available to enterprises across geographies.



Source: Gartner

The elimination of physical constraints, while have eased out the processes, also amplified the countervailing concern of data accessibility and transferability with no restrictions. The concept of global village, that has erased the geographical boundaries, draws no limitations to the data transfer. De-territorialisation and outsourcing of operations and data keeping to providers offshore, is an aftermath of this.

Thanks to offshoring being a necessity in today's cost sensitive industry, the service providers have ready access to client information. Snowden revelations have created a buzz in the industry and added a heavy weight to the term Data Sovereignty. For Service Providers with international operations, this has fuelled an uncomfortable situation where their capability to protect data privacy is under scanner.

To emphasize further, data sovereignty is the behaviour of the federal body of a particular country towards the data being generated, located, or transferred over the wire within their law of land.

Is your data private with the provider in a nation that is not yours?

The data being held in an offshore location could be personally identifiable and could cause a reputational damage when accessed outside an acceptable setup. The data, when regulated by the law of a foreign land, where it is hosted, no more guarantees restricted access and data privacy.

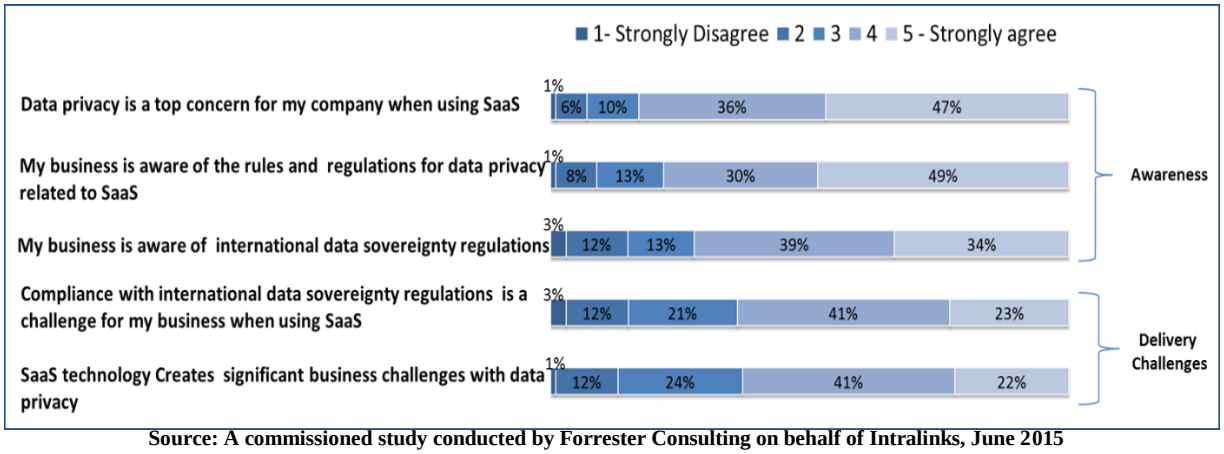
As a learning from the situation in hand, nations in recent times, have come up with some serious data sovereignty laws to see that the plethora of sensitive and business critical data stored on physical and virtual platforms, across nations is secure from foreign surveillance.

Problem Statement:

With internet being the way of life, cross border data flow is an outcome of anywhere-anytime proliferated access.

In a world characterised by globalisation, and as enterprise data migrates geographies, ignoring the risk involved in off shore data keeping, can cause immense damage to customer data privacy.

With data privacy taking the center stage, the lack of homogeneity in the existing data protection laws and governance framework, across nations could act as a reason in inhibiting enterprises from adopting full scale cloud.



Source: A commissioned study conducted by Forrester Consulting on behalf of Intralinks, June 2015

Detail:

The fact that the jurisdiction of any law of land applies only within its territory is what protects the theory of data sovereignty.

Post the Snowden revelations, a wide range of approaches around laws on data privacy and security, have emerged for nations to take a serious stock of.

United States sees the phenomenon of data sovereignty as a threat to open and global internet culture. This view has resulted in multiple instances where questions on privacy intrusion were risen. One such is Germany terminating its contract with Verizon in lieu of the threat to their information.

The ruling of United States against Microsoft Corporation, that the data hosted outside the country can be legally accessed, questions the data privacy and security assurance that any client would want as a part of the service. This has raised alarm amongst the service providers and the client fraternity globally.

The reluctance of Canadian Government to store its information in the United States was addressed by Microsoft through an all new onshore datacenter plan.

The well-defined regulations in the European Union (EU), to promote data privacy and sovereignty, have generated a necessity for service providers to build infrastructure and operate from within the geographical boundaries of EU.

The feasibility of datacenter localisation resulting to data localisation as a solution to this issue is gaining momentum and is being seriously deliberated upon.

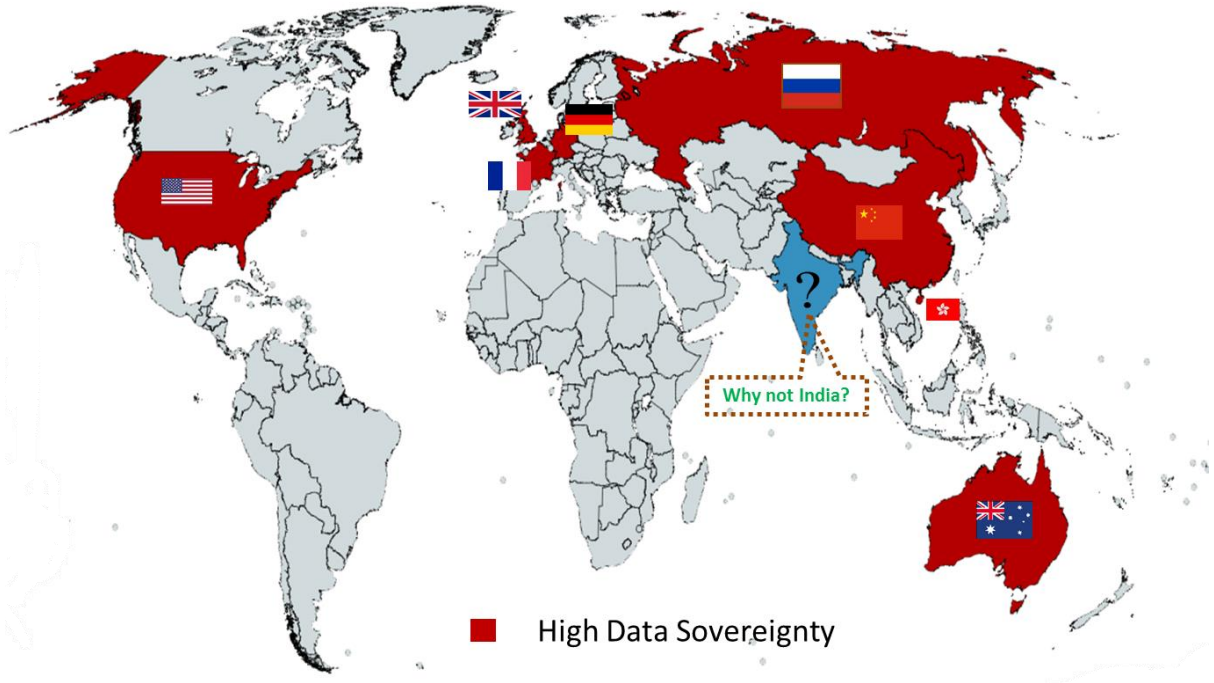
Countries like Russia, Germany, and China advocate that data localisation and local data sovereignty is a must to secure any sensitive national data and data of its nationals.

Data sovereignty has come to prominence in the form of Russian data localization legislation.

China's personal information protection laws on cross-border data transfer are one of the strictest, covering sectors dwelling into personal financial, credit reference and health information. The same laws are being suggested to cover IT and cloud computing. Offshore media data transfers, containing information related to national security and national interests are restricted under Law on Protecting State Secrets. Counter-Terrorism Law are being debated and realigned to bring in Internet and telecom sectors to store data onshore and provide encryption keys to concerned authorities for privacy protection and security.

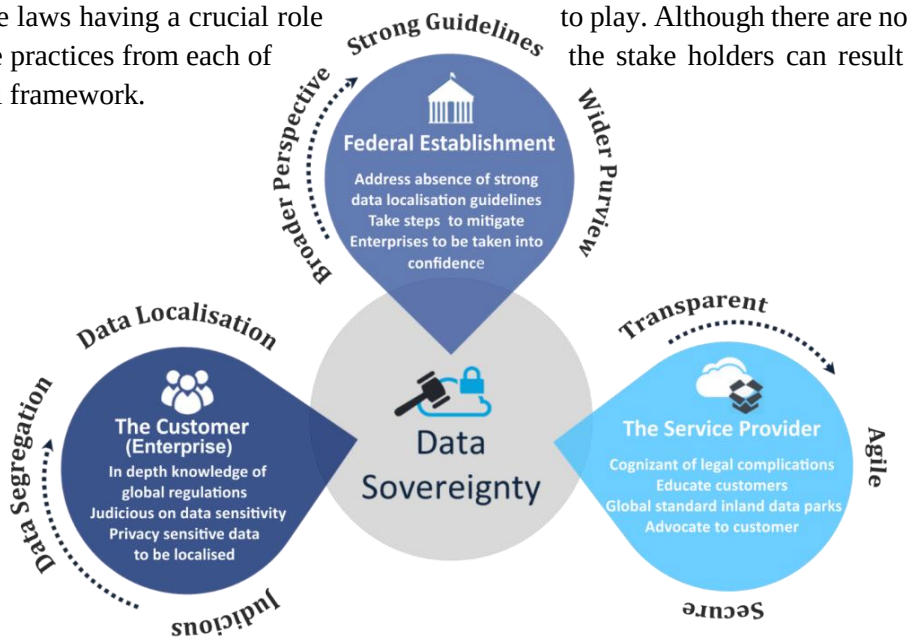
While United States heavily lobbies for open and global internet culture, they have been stringent with their laws in implementing data localisation to protect data privacy for their nationals.

The Australian principles of data sovereignty and privacy have been evolving with the advancements in technology. The amended principles are much tighter towards any offshore service provider for an Australian enterprise, being compliant of Australian Laws in all possibilities. This would make the enterprises consider hosting within the nation, on a serious note.



Certain industry studies talk about approximately 97% of UK, France and Germany based clientele would prefer to contract with European service providers. It stands at 67% for Hong Kong/APAC customers who would prefer to work with Asia Pacific service providers only. 92% of US based customers flagged off US based service providers as their primary pick.

The direct impact of the whole discussion is on customers and the service providers, with the federal bodies and the laws having a crucial role to play. Although there are no defined set of rules, some practices from each of the stake holders can result in a better and beneficial framework.



The Customer's (Enterprise) Role:

- To have an in depth knowledge of laws and regulations depending on the geographical scope and requirements of their business
- To be able to judiciously segregate data, basis its privacy sensitivity and business criticality
- Highly privacy sensitive data of national interest, end user data around personal identity, medical, finance, so on and so forth should be local to the extent possible, ensuring a local jurisdiction

The Provider's Role:

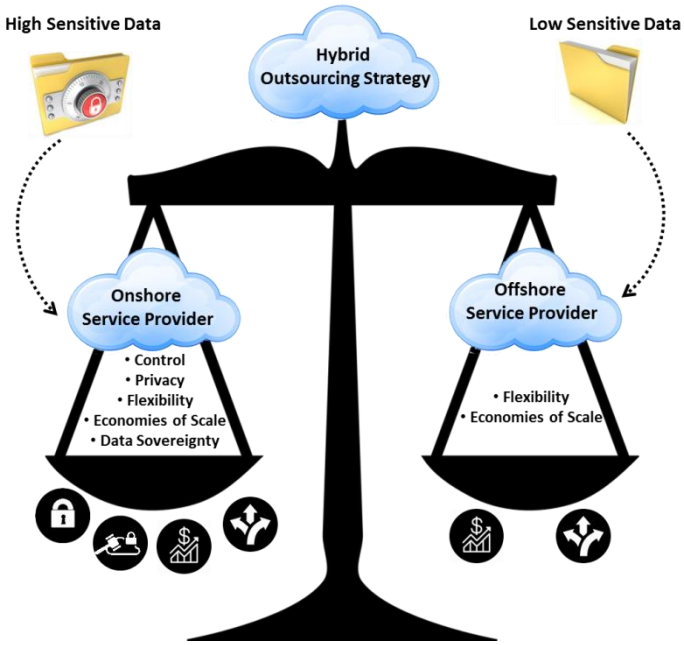
- Cognizant of the legal complications involved
- Proactively educate customers on the implications
- To build a transparent, agile, flexible, seamless and secure environment of services
- Deliver onshore enterprise class data parks at a cost at par if not less to global standards
- Sell enablers aligned to customer's business and not shelf products
- Last but not the least, be an advocate to customer and not a vendor

The Federal Establishment's (Govt.) Role:

- Be cognizant of the magnitude of risk in data privacy pilferage in absence of a strong data localisation guideline
- Have a broader perspective to the threat applicability of data sovereignty is beyond data of national security
- To bring enterprises in Banking, Financial, Insurance, Healthcare, Identity Management verticals under the purview of data localisation, in order to mitigate risking foreign access to private data of its nationals which are resting with these enterprises

Conclusion:

With the booming cloud culture and the exponential data generation globally, service providers should regard the issue with utmost importance.



A nuanced analysis as a part of strategy for any enterprise (private or government) about what data can be stored where and with whom, is the need of the hour. Location and jurisdiction of sensitive data is of high importance.

Any establishment leveraging offsite data parking, should imbibe a new and broader perspective towards data sovereignty, national residency and data localisation.

"A hybrid outsourcing strategy, in line with privacy sensitivity of the data, can address this bone of contention. While to ensure local jurisdiction, hosting highly sensitive and business critical information/data with an onshore datacenter provider is a redressal, offshore hosting could be opted for non-critical and non-sensitive data."

An equilibrium maintained between both the models would transpire to be operationally scalable, secure, economically feasible, yet defying the fall outs of data sovereignty for federal establishments, enterprises and last mile users.

Caveat emptor

(Let the buyer beware)