

**20210412 Atmanirbharta & MEITY decision to permit Government Data Storage in Google Cloud**

**To,**

**Shri Narendra Modi Ji**

**Hon'ble Prime Minister of India**

**Government of India**

**7, Lok Kalyan Marg, New Delhi**

**New Delhi – 110001**

12 April, 2021

Dear Sir,

At the outset, may we thank you Prime Minister, for announcing reforms mandating the prioritisation of domestic procurement, notably leading to revocation of the BSNL 4G tender favouring Chinese companies. **Such steps will turn the tide of India’s fortunes, as it is estimated that domestic procurement by Government can impart a 40% stimulus to GDP, thus turbo-charging economic/technological development and employment, which is Prime Minister’s goal.**

2. In the same vein, we would like to highlight the opportunities and some threats in the thrust towards storing Government Data on Cloud, in light of recent pronouncements by MEITY. The continued thrust on optimising Government IT usage to provide the greatest level of service to the common man indeed mandates the shift to the Cloud. **However,** **it must be taken into account that** **the Cloud is the platform on which sensitive Government Data will be stored and Applications will be developed.** **Thus, it is of critical importance that GoI control the Cloud services used by Government departments/ Government funded projects.**

3. Google has recently proclaimed that it has received GoI/MEITY approval to permit storage of Government data in Google Cloud. This is a disturbing decision with serious security, economic and strategic implications. **It undermines the AtmaNirbharta thrust that has been personally kickstarted by Honourable Prime Minister**. A brief on the implications is summarised below, though the larger picture has been recognised by the Government itself elsewhere.

4. **Big Tech Assuming Dominance over National Governments**: India is no stranger to the power of Big Tech (Facebook, WhatsApp, Twitter in recent times and Google/YouTube earlier). This has been highlighted elsewhere, and in the interest of brevity, a separate overview of actions being taken in the United States, the EU and ***even China*** to counter the enormous power deployed by Big Tech is placed at the Annexure. **Allowing such foreign entities power over Government data, processes and applications will give them even greater leverage in an increasingly asymmetrical situation already fraught with enormous risks for State Sovereignty and Security. India cannot afford to trust foreign providers of such services. For example, 40% of cyber-attacks on India are reportedly attributed to China. The rest are coming from elsewhere. It is imperative that indigenous Clouds, which are already present, be used for such sensitive work.**

5. **National Security Implications: A foreign-owned Cloud will control sensitive Government data, something no independent, proud country can afford or tolerate**. Military practitioners and experts are all agreed that weapons systems will henceforth incorporate Artificial Intelligence (AI) and include unmanned / autonomous systems as key force multipliers. **Military AI in particular will have to draw on indigenous resources including massive bandwidth, indigenous Clouds, the 5G core, Servers, data centres and advanced hardware for the super-fast communications essential for real-time military operations.** Moreover, there are no wars that are now confined to militaries: **the nation as a whole is both under attack and part of the response as ICT networks are indivisible**. **If the Cloud, ICT networks and data stores are owned by foreign entities, India’s ability to conduct even its military affairs independent of any pressures will be severely compromised and reduced**. We cannot allow entities subject to foreign regulations and extra-territorial pressures - business or political - whether the EU or the US, control the availability and breach the confidentiality of the Indian Government’s operations in the Cloud. Once such entities have access, or indeed control of our cloud, **regulations that dictate storage of data in India etc. are unenforceable and indeed not auditable. This is in direct contravention to MEITY’s own policy on Cloud Service Providers** **which states that: “*all services including data will be guaranteed to reside in India.”* (**[**https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual\_Terms.pdf**](https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf)**)**

6. **Economic Security Implications:** The term Cloud itself is rather a misnomer. Google advertises itself as the Google Cloud Platform; Amazon as Amazon Web Services, and Microsoft as Azure Cloud Computing Services. It is therefore evident that the Cloud provider is essentially the Application Development Platform. **The economic consequences of giving Google permission to host Government data will mean that Google (and no doubt in quick succession Azure/AWS) will become the preferred development platforms for all industry**. **This will be the death knell for Indian IT Industry’s attempts to ascend the value chain**. Google (and similar entities) will invariably swallow Indian companies, data centres and cloud providers as they will be unable to offer matching terms. Google can even offer to host Govt data for free and profit from the **massive meta-data monetisation opportunities**! All subsequent applications will be developed on Google Cloud Platform, rather than on Indian IPR. The Atmanirbhar dream of Making in India for The World will be reduced to outsourced labour for MNCs that will continue to dominate all revenue models.

**Conclusion**

**A strong ICT industry is India’s force multiplier for National Security. Moreover, a*ll future technological progress will depend on mastery of ICT technologies*. Our Government is committed to the National Security and economic development of the country. India must therefore ensure that ICT networks which includes the Cloud - are treated as an indivisible whole, and the nation’s Super-Critical, Sensitive and Strategic Information Infrastructure protected through indigenous capabilities. National Security Agencies, capable of taking a holistic view of issues affecting the nation’s security and integrity, must be involved in comprehensive internal reviews before critical decisions by line Ministries affecting the integrity, resilience and security of India’s Critical Information Infrastructure are taken. We humbly request a formal audience to list our critical recommendations in this regard.**

**For the present, we would strongly urge the Honourable Prime Minister’s intervention to see that the MEITY pronouncement giving departments leeway to use Google Cloud, and indeed all pronouncements related to Big Tech and Big 4 Consultancies, must be strictly be in conformance with laid down policy and withdrawn and not implemented if not so conformant.**

With kind regards and best wishes,

Smita Purushottam

Chairperson SITARA / Ambassador (Rtd.)

The Science, Indigenous Technology & Advanced Research Accelerator

**Annex**

**Worldwide Concerns over Big Tech**

**US and EU measures**

Common US/EU issues with Big Tech: anti-competitive, antitrust behavior/ suppressing innovation and start-ups by shutting out or buying out rivals, driving small companies to bankruptcy, illegal content, disinformation, influence operations, information monopolies, preferential treatment to own products, oligopolies, monetization of data leading to worries about privacy and data misuse.

**United States**

As a result of growing concern, bipartisan antitrust investigations have been launched at the Federal and State levels in the U.S.. A Congressional report has concluded that Amazon, Apple, Google and Facebook have abused their market power through “a series of anti-competitive business practices” and provided **46 pages of smaller, high-tech companies taken over and suffocated by Big Tech** (<https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf>)! The U.S. Justice Department is suing Google for illegally abusing its dominance over smaller rivals, and stifling competition, using profits made from its monopolies “to buy special treatment for its search engine on devices and Web browsers, creating what the department says is a "self-reinforcing cycle" of monopoly power abuse”. Action to constrain abuses of power by Big Tech is under consideration.

**EU**

Germany and France are already implementing rules to restrain Big Tech, not wishing to wait for the EU’s cumbersome processes: Germany on antitrust, France on disinformation and hate speech. France had also pushed forward on new taxes causing a major clash with the U.S.. Angela Merkel has urged the EU to claim ‘digital sovereignty’ by developing its own platforms and reducing its reliance on Amazon, Microsoft and Google. Margrethe Vestager, the EU’s competition chief who in in charge of EU digital policy, is also spearheading efforts at the EU level to control Big Tech. On Dec 15, 2020, the EU proposed the Digital Services and Digital Markets Acts, which could fine (up to 10 percent of global business turnover, or $28 billion in Amazon’s case) and even break up Big Tech companies for abuse of market power.

European regulators also want to designate Cloud, data-centres and related sectors as critical infrastructure.

**China and Big Tech**

The power of China’s Big Tech Titans - Alibaba and Tencent - has rattled even the powerful Chinese Communist Party. Xi Jinping’s order to **suspend Ant’s $37 billion IPO and levy a US$2.8 billion anti-trust fine on it was part of an effort to humble Big Tech**. China has issued new and comprehensive guidelines to prohibit monopolistic, anti-competitive, exclusionary practices, price fixing, restricting technologies and using algorithms for market manipulation.

Meanwhile, Big Tech has no qualms about bowing to China’s dictates. In 2018 Facebook confirmed they had entered into data sharing partnerships without the explicit consent of FB users with several Chinese companies including Huawei. Apple censored content and apps objected to by the Chinese Govt. Apple also outsourced its iCloud operations to a Chinese cloud provider with close ties to the Chinese Government, which transferred user data to China Telecom, a state-owned company. Apple is also lobbying against a bill aimed at stopping forced labor in China. Former US Attorney General William Barr complained that US companies were only too willing to collaborate with the Chinese Communist party for market access, with Hollywood “routinely caving into pressure and censoring their films to appease the Chinese Communist Party.”

**Big Tech threatens Nations**

Big Tech’s power rivals that of Governments themselves today. Google recently threatened to remove its search engine after Australia tried to make payment for news content mandatory. We have seen what kind of power Twitter recently exercised in the US presidential campaign and even in India’s domestic politics. It is not in our national interest to alienate so much power and control to Big Tech. in fact some arms of the Indian government are taking steps to constrain the power of Big Tech so MEITY’s decision goes against Government policy.

**India and Big Tech**

Surprisingly, MEITY does not seem to be aware of the gathering disquiet within Government circles over the monopoly and anti-competitive behaviours of Big Tech in India. Government has been trying to ensure a fair market for India's smaller retailers, which accuse foreign ecommerce giants of unfair business practices including steep discounts to push them out of the market. In fact, after Amazon was kicked out of China, it had no choice but to concentrate all its focus on the Indian market to the detriment of local players (Flipkart had requested Government support to face Amazon’s onslaught). Internal Amazon documents have revealed its shady strategy to dodge India regulators favouring big sellers on its India platform. Shri Piyush Goyal has rightly said that Amazon is not doing India any favours by investing here. Even FICCI has recently disowned Amazon’s representations to Government stating that the laws of the land have to be strictly observed by any company. The Enforcement Directorate is also investigating Amazon for violations of FDI rules and the CCI is looking into Google Pay’s exclusion of other payment apps from Google app payments. These, including India’s equalisation levy and moves towards data privacy have predictably drawn the ire of the USTR which has recommended retaliatory action. India has also objected to WhatsApp’s changes to its privacy policy.

\*\*\*\*