ispirt

SITARA

**To**
**Shri P.K. Mishra**
**Principal Secretary to PM**
**PMO, South Block, New Delhi, 110011**

Friday, 26 September 2025

**Subject: Urgent Need for a Digital Sovereignty Law**

Dear Sir,

At the outset we wish to record our appreciation for the welcome steps taken by Government to catalyse a high-tech, indigenous digital ecosystem through initiatives such as the **Digital Public Infrastructure (DPI), Jan Dhan, Aadhaar, UPI, the National AI and Quantum Missions and the Semiconductor Mission.** Additionally, the RDI initiative with significant funding for the private sector, has the potential to revolutionise India's R&D landscape.

2. In the Free Trade Agreements (FTAs), India has rightly kept sensitive sectors such as agriculture, dairy, and genetically modified products out of bounds. However, concessions on source code access, cross-border data flows, open government data, local presence, and prohibitions on digital custom duties - risk undermining India's digital sovereignty. Additionally, while the free movement of skilled workers and the H1B visa issue are important, they cannot justify yielding on India's core digital interests. These concessions are already apart from the asymmetrical access to India's public procurement system and the preference for voluntary licensing in the FTA texts already conceded in the UK FTA. At a time when the United States is taking extremely unreasonable steps aimed at extracting further concessions, accepting such terms could derail India's ambition to emerge as a global Digital Power.

3. The Nayara case, where Microsoft and SAP withdrew essential cloud services due to EU sanctions, also illustrates our vulnerability. Indian courts, *lacking the legal framework for holding global digital companies accountable*, refused interim relief for Nayara. Earlier, on being summoned by the Supreme Court of India regarding content regulation issues, Google India had deflected responsibility to its US parent.

**Strategic Imperative**

4. All the above highlights the urgent need for a **Digital Sovereignty Law** defining Indian authority over all digital actors and infrastructure within its jurisdiction and a **Digital Industrialisation Strategy** to expand Indian capacity. Ironically, the United States —whose Big Tech companies have transgressed digital sovereignty around the world, prompting constant alarm in the EU—has also evolved the best model for sovereign oversight. Washington recently initiated the forced divestiture of Tik Tok, ring-fencing TikTok from its Chinese parent, subjecting algorithm use to domestic control/ royalties, and confining sensitive operations to transparent "clean rooms". Thus, powerful foreign tech giants can be forced to comply with national rules when governments act decisively, although it is not

always necessary to uniformly follow the US template of complete ownership change, only for ‘local presence’ with specified conditions.

5. India, with its vast market and rapidly expanding digital economy, cannot allow foreign digital platforms to siphon off Indian data and profits and potentially weaponise it, while hiding behind foreign jurisdictions. **China’s US$2 trillion digital economy demonstrates the concrete benefits of digital sovereignty. In contrast, India’s digital exports, valued at US$220 billion, largely generate trillion-dollar profits abroad for foreign companies**, with Nvidia’s valuation quadrupling in two years to US$4 trillion, with limited domestic multipliers. The bulk of Nvidia’s engineering workforce is from India.

6. India should therefore develop its own approach on Digital Sovereignty, requiring foreign entities to operate through subsidiaries incorporated here subject to Indian law, audits, and enforcement. Violations must carry penalties like heavy fines, suspension or expulsion. **The Indian Government must move high risk sectors containing critical data in DigiLocker, GeM and the national highways data repositories and any other critical data - to sovereign indigenous Indian Clouds and ensure that foreign clouds do not misappropriate the term “sovereign”. It must be borne in mind that US companies are required to share any data they hold anywhere in the world with the US Government as per the Cloud and FISA Acts, on top of other executive orders and requirements.**

7. India can also take appropriate lessons from all around, enlisting allies like the EU and the bigger developing countries like Brazil, South Africa, and Indonesia, who are all deeply concerned about their digital sovereignty. This is a good place for India to exhibit its *Vishwaguru* leadership. We are convinced that this can be done while maintaining India’s economic and political relationship with its key allies, as also retaining the best digital services for its people.

8. As PMO is aware, national power increasingly rests on technological capability, which in turn depends on a robust foundational digital ecosystem. Without immediate action, India risks a systemic erosion of its digital industrial base, with the net effect being crippling India as a viable economy, unable to make sovereign choices. **We appeal to Hon’ble Prime Minister that this be taken up urgently at the highest levels before any more concessions are made which could lock India into digital subservience in perpetuity - and a Digital Sovereignty Law applying Constitutional principles to the digital realm be enacted. Because as per our Constitution, the Indian Republic exercises unquestionable sovereignty, power and authority, answerable to none.** India cannot repeat past errors of allowing foreign platforms to entrench themselves before laws on digital sovereignty ensuring that foreign firms operate on India’s terms - are passed.

9. The time to act is now. India’s technological and economic future, as well as its strategic autonomy, depend on it. We thus urgently appeal that Government:

I. Launch a **Digital Industrialisation Strategy** to develop sovereign cloud, apps, platforms, mobile and enterprise OS, and the corresponding hardware stack.

II. India enact a **Digital Sovereignty Law**.

Details are at Annex A.

**Respectfully,**

Sharad Sharma

Amol Khire

Parminder Jeet Singh

Abhijit Das

Abhishek Bhatt

Rajeev Srinivasan

Ayonam Ray

Nivedita Haran

Ashish Sonal

Smita Purushottam

**iSPIRT/**

**SITARA**

**Annex A**

## I. Digital Industrialisation Strategy

- Government must encourage the development of a sovereign technology stack including cloud infrastructure, social media platforms and apps and shift its data (DigiLocker, national highways data, GeM etc) to indigenous Clouds.
- Government procurement should prioritize domestic digital products.

## II. Digital Sovereignty Law.

A Digital Sovereignty Law based on a risk-based approach is proposed. It prescribes and enforces the safeguards needed to maintain Digital Sovereignty:

- **High Risk:** Government cum Citizen Services, critical applications for economy, social media - need to be fully ring-fenced and comply with more stringent provisions of the law
- **Medium Risk**: non-critical Govt Apps, Corporate Applications will safeguard data security, business continuity and access to justice.
- **Low Risk areas**: Lower safeguards with the intent to allow free market expansion of digital services from global players in India.

### 1. Legal Jurisdiction and Local Presence

- All foreign digital service providers above a high threshold of business/ clientele must establish a legally incorporated, operationally independent Indian subsidiary, responsible for all its Indian operations, including service continuity and compliance with Indian laws. No accountability can be shifted to the foreign parent.

- Large digital platforms must separate Indian operations from their global infrastructure.

- Critical infrastructure services—cloud platforms, operating systems, enterprise software—must operate under licensing regimes akin to telecom, ensuring neutrality, transparency, interoperability and regulatory oversight.

- The definition of sovereign clouds must pre-empt the appropriation of the term by foreign entities which are increasingly using the term "sovereign" loosely to describe their India-based operations.

**2. Ownership Transparency**

- Companies must disclose Indian shareholding structures and changes in majority ownership will require regulatory approval.

- The right to sell IP to foreign entities should be regulated to prevent undue foreign acquisition of successful critical Indian technology.

3**. "Systemic" service providers** (service providers that are so large or essential to the ecosystem that their services are considered critical for the functioning of the market/society):

- Algorithms, data, and other critical processes must run in transparent "clean rooms" subject to independent audits, ensuring no foreign entity can unilaterally control or manipulate services.

- Digital auditors, akin to professional bodies like ICAI, should be established to monitor compliance.

**4. Interoperability and Unbundling**

- Systemically important providers must allow , and enable, smaller cloud companies and service providers to run their software or hardware on the systemic provider's infrastructure - servers, network, or storage.

- Third-party audited APIs and technical documentation must be provided for this purpose, following models like the EU Digital Markets Act and AI Act.

**5. Transparency of Digital Value and Data**

- Mechanisms must be developed to trace the value created by Indian data, algorithms, and AI, including outflows to foreign entities.

- This framework will support taxation, prevent unfair profit repatriation, and ensure equitable economic gains from digital assets.

- Profits may be repatriated only after full compliance with Indian laws.

## 6. Regulation of Digital Advertising and Monopolistic Practices

- Digital advertising should be taxed at higher rates to capture excess profits from monopolistic targeting.

- Anti-competitive practices, such as predatory pricing or loss-leader strategies, must be prevented.

## 7. Protection of Critical Rights

- Indian law must guarantee algorithmic transparency, prevent backdoors, and prohibit intentional shutdown mechanisms.

- Source code audits must be conducted by independent, certified third parties.

- All critical data must reside in India, with strict rules against foreign transfers

Friday, 26 September 2025.