The Illusion of Sovereignty: Exposing the Discrepancies in "Make in India" Tech

An Investigative Report on the AI Plus Smartphone Controversy, Geopolitical Marketing, and Systemic Vulnerabilities in Domestic Electronics Manufacturing

Subject:	AI Plus Smartphone Investigation & "Make in India" Discrepancies	**Date:**	July 8, 2026
Source Material:	"I Investigated India's Biggest Smartphone Controversy" (Mrwhosetheboss)	**Context:**	Tech Nationalism, Legal Overreach, and Supply Chain Realities

1. EXECUTIVE SUMMARY

In recent years, India's push for technology sovereignty under the "Make in India" banner has intensified, fueled by a desire to capture a slice of the world's second-largest smartphone market (boasting over 700 million users). This report deconstructs a severe and illustrative controversy involving **AI Plus**, a prominent domestic consumer electronics brand launched in July 2025. Led by industry veteran Madhav Sheth, AI Plus aggressively marketed its devices as India's first "fully sovereign, expertly engineered, and meticulously built" smartphones, explicitly weaponizing anti-Chinese sentiment and hyper-nationalistic narratives to drive adoption.

However, an open-source investigation by the tech community revealed a systematic breakdown of these claims. Far from being indigenous, independent audits uncovered that AI Plus devices are rebadged Chinese reference designs sourced from low-tier Original Design Manufacturers (ODMs), containing un-installable Chinese spyware, hardcoded Chinese firmware permissions, and recycled secondhand hardware components. To suppress these findings, AI Plus manipulated the Indian legal framework, securing aggressive *ex-parte* gag orders to silence domestic journalists. This case exposes a stark reality: behind the patriotic marketing of some "Make in India" tech lies an absolute dependence on the cheap, unvetted Chinese supply chains they publicly claim to replace.

2. THE ANATOMY OF GEOPOLITICAL MARKETING

The Indian smartphone sector is heavily dominated by Chinese brands such as Xiaomi, Vivo, and Oppo, which collectively command over two-thirds of the market share. To exploit this structural

imbalance, AI Plus entered the market with an unnuanced, explicitly political campaign. Central to its brand thesis were three specific promises:

- **Data Sovereignty:** The company explicitly promised on its boot screen: *"Your data stays safe in India,"* alleging that all user telemetry would be securely localized within Google Cloud India regions.
- **Software Integrity:** The brand marketed its proprietary skin, *Next Quantum OS*, as an indigenous development. The CEO publicly declared that "Made in India means little if software and updates come from abroad," throwing direct shade at rival domestic assemblers like Lava, Micromax, and Karbonn.
- **National Security Cleared:** AI Plus claimed its phones were so hardened and secure that they were "certified for government use."

This reached a peak with a cartoon-strip style advertisement depicting an Indian consumer waking up to a fraudulent loan taken out in his name, with the culprit explicitly depicted as a malicious caricature of a Chinese citizen. This hyper-aggressive positioning set a benchmark of accountability that the company's underlying engineering failed to sustain.

3. UNMASKING THE DISCREPANCIES: THE INVESTIGATION

Independent technical deep-dives conducted by digital forensics and tech reviewers shattered the illusion of an indigenously developed ecosystem.

A. The Software & Firmware Facade

When independent software analysts decompiled the code bases of the pre-installed system applications on AI Plus devices, they discovered systematic rebadging:

- **Next Quantum OS:** Instead of being an indigenous operating system built from scratch, the user interface was mathematically and visually identical to Realme's operating system—the Chinese brand previously helmed by Sheth.
- **Hardcoded Chinese Backdoors:** Critical system utilities that users are prohibited from disabling or deleting—specifically *Clean Assistant*, *Phone Clone*, and *Mobile Butler (Phone Manager)*—were found to be wholly authored by **Sprocom Technologies**, a software and hardware ODM based in Shenzhen, China.
- **Extensive Telemetry:** Forensic inspection of the privacy policy built into these system apps revealed explicit declarations that user information would be collected directly, automatically, and from "other sources," under the service provision of Chinese entities, fundamentally invalidating the "data stays safe in India" mandate.
- **ZTE Firmware Integration:** In higher-end hardware such as the *Nova Flip*, decompiled system images showed that fundamental system services—including the default compass app,

the core fingerprint biometric framework, and the device's integrated AI Engine—were littered with explicit, unmasked ***ZTE*** identifiers, operating with 20 to 30 deep kernel-level system permissions.

B. The Hardware Shell Game and the Secondhand Component Scandal

The manufacturing discrepancies extend deep into the hardware assembly. Supply chain audits reveal that AI Plus operates entirely through an ODM model rather than a contract manufacturing model. While an organization like Apple designs proprietary chips and layouts and leases factory lines to build them, AI Plus purchases off-the-shelf reference designs from low-tier Chinese ODMs (such as Sprocom and Lee Fine Technology), applies cosmetic modifications to the rear plastic casing, and laser-etches its corporate logo on the exterior.

> **The Economics of Low-Tier ODMs:**
>
> According to high-level Indian electronics supply chain whistleblowers, low-tier Chinese ODMs maintain razor-thin margins by slashing engineering costs and sourcing **recycled, secondhand components**. A critical discrepancy highlighted involves memory chips. While a new, un-used 64 GB flash storage module commands a market price of roughly $P_{new} = \$60$, low-tier ODMs frequently harvest used chips from decommissioned electronics, integrating them into "new" phones for as low as $P_{used} = \$20$.

This reliance on harvested components introduces massive quality control failures. Batch tracing becomes statistically impossible, explaining why thousands of retail customers in India remain permanently stranded on outdated, vulnerable December 2025 firmware builds, entirely cut off from security updates. Furthermore, products marketed as "designed and patented in India," such as the AI Plus *Wearbuds* (a smartwatch containing integrated wireless earphones), were discovered to be a absolute clone of products developed years prior by a Chinese firm named *AI Power*. The corporate logos are so interconnected that the "AI" vector graphic from the AI Plus logo overlays seamlessly onto the Chinese company's asset.

4. WEAPONIZING THE JUDICIARY: THE LEGAL INJUNCTIONS

When prominent Indian tech journalists (including channels such as *Techweiser*, *Techbar*, and *Gyan Therapy*) published documented video evidence of these Chinese backdoors, missing updates, and cloned hardware, AI Plus responded not with a technical refutation, but with legal warfare.

The company bypassed standard civil litigation protocols to secure an **ex-parte injunction** from the Delhi High Court. In an ex-parte proceeding, the court hears arguments exclusively from the

plaintiff, without the presence or knowledge of the defendants. To execute this legal maneuver, AI Plus utilized specific procedural tactics:

1. **The "John Doe" (Ashok Kumar) Precedent:** AI Plus designated an unnamed entity, "John Doe," as the primary defendant in the lawsuit. Under Indian procedural law, this allows a plaintiff to bypass the absolute necessity of serving an advanced warning notice to the actual targeted individuals, under the legal fiction that the primary culprits are unidentified.
2. **Deceptive Service Protocols:** For the actual named creators (e.g., Techweiser), the company transmitted the mandatory legal notices to intentionally fabricated, non-existent email addresses—despite having historically communicated with the creators' genuine press addresses days prior. This effectively prevented the journalists from mounting an immediate legal defense before the temporary gag order was executed.

   By the time the creators discovered the litigation, an emergency gag order had been issued, forcing the immediate geoblocking and deletion of over a dozen critical investigative videos. This legal manipulation created a highly asymmetric power dynamic, leveraging millions of dollars in corporate capital to completely suppress factual consumer tech reporting during a critical commercial product launch window.

5. SYSTEMIC IMPLICATIONS FOR "MAKE IN INDIA" TECH

The AI Plus crisis serves as an indictment of structural loopholes within the current domestic electronics ecosystem. It highlights a critical systemic divergence between true, deep-tech domestic industrialization and superficial assembly-driven nationalism:

> *"Made in India cannot simply be a cosmetic layer applied over unvetted, foreign-designed blueprints. When nationalistic sentiment is leveraged as a primary marketing tool to shield sub-standard, insecure engineering from criticism, it actively undermines long-term industrial credibility."*

Currently, the "Make in India" framework relies heavily on Phased Manufacturing Programmes (PMPs) that incentivize local assembly (SKD/CKD kits) via tariff structures. However, because the underlying intellectual property (IP), Printed Circuit Board (PCB) routing, kernel source code, and firmware architectures remain entirely anchored in Shenzhen, true strategic sovereignty is non-existent. When domestic brands choose low-tier Chinese partners to maximize profit margins while wrapping their products in the national flag, they do not just deceive consumers—they introduce profound data security vulnerabilities directly into the pockets of millions of citizens.

References & Source Attribtion:

This document compiles and structurally analyzes the investigative data, firmware extractions, supply chain interviews, and legal filings detailed in the video report *"I Investigated India's Biggest Smartphone Controversy"* by Mrwhosetheboss (Published May 30, 2026). Digital tracking ID for verification: `gmail_search_query: "Mrwhosetheboss AI Plus smartphone controversy India tech investigation 2026"`.