

Smartphone Source Code: Government Debate and Security Concerns

January 14, 2026 • vajiramandravi.com



Smartphone Source Code Latest News

- A Reuters report claimed that the Indian government was considering requiring smartphone manufacturers to share their source code with third-party testing agencies and inform authorities before major software updates.
- However, the Union government has downplayed these discussions and denied any proposal to demand disclosure of source code.

About Source Code

- Source code is the foundational set of instructions and digital assets that power a software system.
- In simpler terms, the source code is highly confidential data that controls the device's memory, processor, sensors, and hardware features.

- While parts of platforms like Android are open-source, manufacturers make extensive proprietary modifications that they closely guard.
- Source code is protected not only for commercial reasons but also for **security**, as exposing a system's inner workings could allow malicious actors to identify vulnerabilities, leading to data breaches and cyberattacks.

Why Source Code Disclosure Is Highly Unusual

- Disclosing source code outside a company is extremely rare and usually limited to sensitive sectors like defence, and even then only in select countries.
- For instance, Apple Inc. has not shared its source code with the Chinese government, despite adopting country-specific policies to comply with local data access laws.
- This underscores how exceptional and sensitive such a demand would be.

Recent Context Heightening the Controversy

- The reports surfaced soon after the DoT faced widespread political and public backlash over its directive to smartphone makers to preinstall the Sanchar Saathi app.
- Critics feared the app could enable surveillance or pose security risks, and global smartphone manufacturers typically resist such preinstallation demands.

Security and Commercial Risks of Source Code Exposure

- Requiring source code disclosure would be far more intrusive than preinstalling an app, as it would expose a company's entire proprietary codebase to third parties.
- **Cyber attackers** usually exploit vulnerabilities visible from the outside; internal visibility would significantly amplify risks, especially if documentation reveals system architecture.
- Even phones running Android do not expose all implementation details, precisely to safeguard security and intellectual property.

Government Position on Public Disclosure of Source Code

- The Indian government has not officially stated that smartphone source code must be made public.
- However, discussions stem from a 2023 document finalised by the National Centre for Communication Security under the DoT, which issued an **Indian Telecom Security Assurance Requirement (ITSAR)** for consumer equipment.

Regulatory Background and Shifting Oversight

- ITSARs form part of the Mandatory Testing and Certification of Telecommunication Equipment (MTCTE) framework, rooted in the Indian Telegraph (Amendment) Rules, 2017.
- However, after the Telecommunications Act, 2023, the government decided to drop MTCTE requirements for smartphones, since they already undergo certification by the Bureau of Indian Standards.
- Oversight subsequently shifted to the Ministry of Electronics and Information Technology, which stated it is keeping an "open mind" on the issue.

Industry and Government Responses

- Industry body India Cellular and Electronics Association has downplayed the seriousness of the discussions.
- Government representatives have also maintained that no final regulations have been framed, suggesting that deliberations are still exploratory.
- The Internet Freedom Foundation (IFF) has challenged these assurances, arguing that ITSAR documents remain publicly available and that stakeholder meetings lack transparency.
- IFF has demanded disclosure of meeting minutes and called for open public consultation, asserting that meaningful policy-making cannot be confined to closed-door discussions with major technology firms.
- The group has reiterated the need for transparency and inclusive consultation in matters that could significantly affect digital rights, security, and consumer trust.

Source: TH | ITV

Source: <https://vajiramandravi.com/current-affairs/smartphone-source-code-government-debate-and-security-concerns/>

© Vajiram & Ravi. For personal use only.