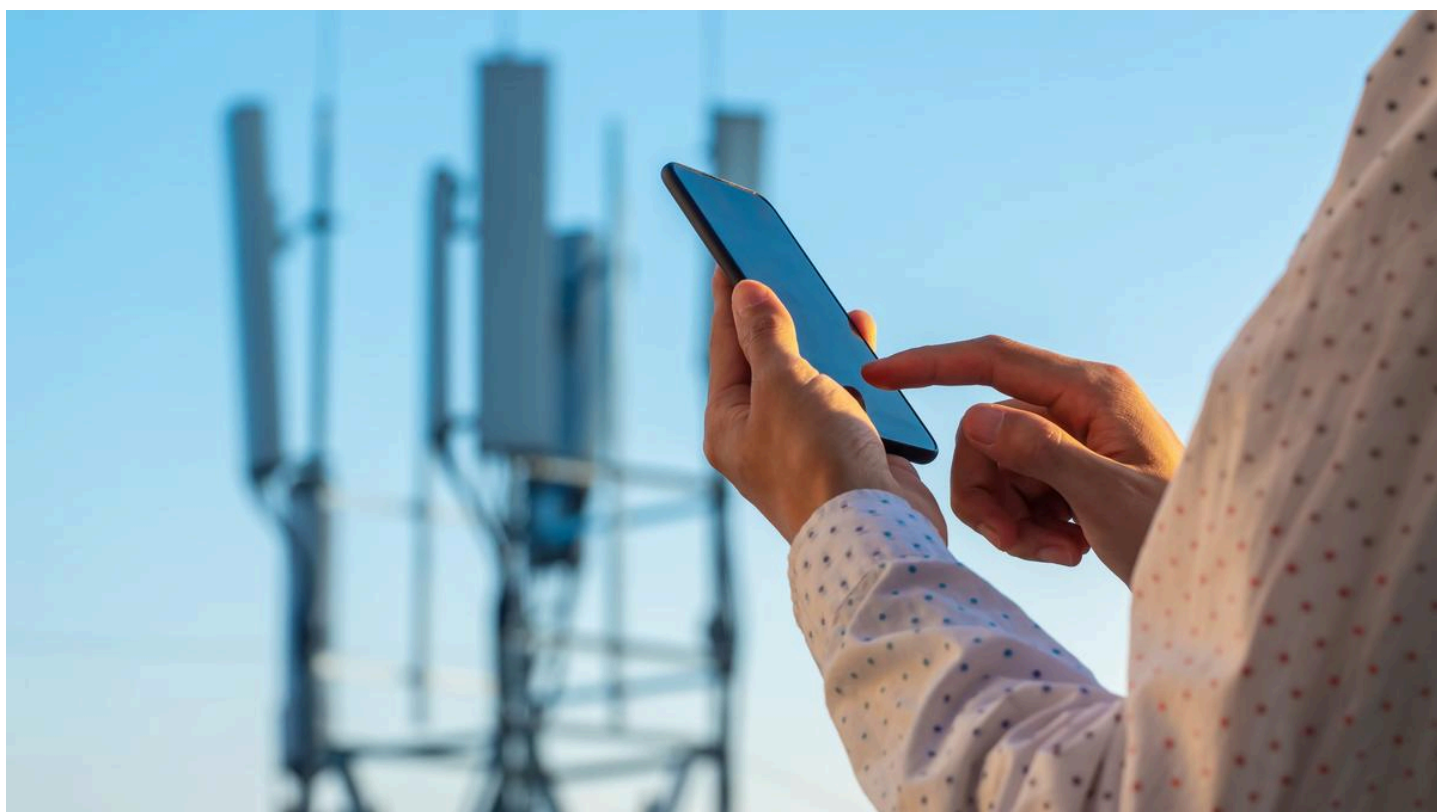# Centre proposes smartphone makers give source code in security overhaul

The plan is part of Prime Minister Narendra Modi's efforts to boost the security of user data as online fraud and data breaches increase in the world's second-largest smartphone market, with nearly 750 million phones

Updated – January 12, 2026 08:18 am IST – NEW DELHI

REUTERS

Among the most sensitive requirements in the new Indian Telecom Security Assurance Requirements is access to source code – the underlying programming instructions that make phones work. (Image used for representational purpose only) | Photo Credit: Getty Images/iStockphoto

The Centre proposes requiring smartphone makers to share source code with the government and make several software changes as part of a raft of security measures, prompting behind-the-scenes opposition from giants like Apple and Samsung.

The tech companies have countered that the package of 83 security standards, which would also include a requirement to alert the government to major software updates, lacks any global precedent and risks revealing proprietary details, according to four people familiar with the discussions and a *Reuters* review of confidential government and industry documents.

The plan is part of Prime Minister Narendra Modi's efforts to boost the security of user data as online fraud and data breaches increase in the world's second-largest smartphone market, with nearly 750 million phones.

IT Secretary S. Krishnan told *Reuters* that "any legitimate concerns of the industry will be addressed with an open mind", adding it was "premature to read more into it". A Ministry spokesperson said it could not comment further due to ongoing consultation with tech companies on the proposals.

Ongoing tug of war over government requirements

Apple, South Korea's Samsung, Google, China's Xiaomi, and Manufacturers' Association for Information Technology (MAIT), the industry group that represents the firms, did not respond to requests for comment.

The Union Government requirements have irked technology firms before. Last month, it revoked an order mandating a state-run cyber safety app on phones amid concerns over surveillance. But the government brushed aside lobbying last year and required rigorous testing for security cameras over fears of Chinese spying.

Xiaomi and Samsung — whose phones use Google's Android operating system — hold 19% and 15%, respectively, of India's market share, and Apple 5%, Counterpoint Research estimates.

Among the most sensitive requirements in the new Indian Telecom Security Assurance Requirements is access to source code - the underlying programming instructions that

make phones work. This would be analysed and possibly tested at the designated labs, the documents show.

The Centre's proposals also require companies to make software changes to allow pre-installed apps to be uninstalled and to block apps from using cameras and microphones in the background to "avoid malicious usage".

"Industry raised concerns that globally security requirements have not been mandated by any country," said a December IT Ministry document detailing meetings that officials held with Apple, Samsung, Google , and Xiaomi.

"The security standards, drafted in 2023, are in the spotlight now as the government is considering imposing them legally. IT Ministry and tech executives are due to meet on Tuesday [January 13, 2026] for more discussions," sources said.

Companies say source code review, analysis, 'Not possible'

Smartphone makers closely guard their source code. Apple declined China's request for source code between 2014 and 2016, and U.S. law enforcement has also tried and failed to get it.

The Union Government's proposals for "vulnerability analysis" and "source code review" would require smartphone makers to perform a "complete security assessment", after which test labs in the country could check their claims through source code review and analysis.

"This is not possible due to secrecy and privacy," MAIT said in a confidential document drafted in response to the government proposal, and seen by *Reuters*. "Major countries in the EU, North America, Australia, and Africa do not mandate these requirements."

"MAIT asked the Ministry last week to drop the proposal," a source with direct knowledge said. The Centre's proposals would mandate automatic and periodic malware scanning on phones. Device makers would also have to inform the National Centre for Communication Security about major software updates and security patches before releasing them to users, and the Centre would have the right to test them.

MAIT's document says regular malware scanning significantly drains a phone's battery, and seeking government approval for software updates is "impractical" as they need to be issued promptly.

The Centre also wants the phone's logs — digital records of its system activity — to be stored for at least 12 months on the device. "There is not enough room on the device to store 1-year log events," MAIT said in the document.

Published – January 11, 2026 03:16 pm IST

In Case You Missed It

'Indian Idol 3' winner and 'Paatal Lok' actor Prashan...

Disinformation is weaponised on social media, says N. Ram

PM should speak on jobs not give history lessons, says...

India should design and manufacture 70% of...

U.S. to push for quicker action in reducing reliance on...

Grok AI issue: X 'accepts its mistake', assures it will...

Biting cold grips Delhi as minimum temperatures...

Countdown for launch of PSLV–C62/EOS–N1 mission begins