

6. INFORMATION TECHNOLOGY SECTOR

6.1 Government to unlock crucial spectrum for high-speed WiFi: What it means for tech companies

In May 2025, India's Department of Telecommunications proposed allowing license-free use of the 5925–6425 MHz band for indoor Wi-Fi, aiming to boost high-speed, cost-effective internet access. This move aligns India with global leaders in 6 GHz Wi-Fi deployment and supports broader digital inclusion.

Refined Reflections:

The Department of Telecommunications' draft proposal to allow license-free use of the 5925–6425 MHz band for indoor Wi-Fi marks a significant step for India's digital infrastructure. With over 850 million internet users and soaring data demand from streaming, remote work, and IoT devices, the existing 2.4 GHz and 5 GHz bands are under immense pressure. By opening up this part of the 6 GHz spectrum, India aims to provide faster, more reliable, and cost-effective wireless internet access, similar to moves already made by countries like the USA, UK, and South Korea. This could greatly benefit schools, hospitals, small businesses, and homes by offering enterprise-grade connectivity without spectrum fees.

This initiative also supports broader national goals like Make in India and Digital India. It encourages innovation in networking hardware and local manufacturing of Wi-Fi equipment, potentially creating new business opportunities. Additionally, by aligning with global standards for unlicensed 6 GHz Wi-Fi, India positions itself as a key player in international conversations around spectrum use and internet access. The move could democratize high-speed connectivity for MSMEs and startups that cannot afford expensive leased lines or 5G setups, helping to bridge the digital divide.

However, the proposal faces challenges. The 6 GHz band is currently used by satellite and fixed-service license holders, raising concerns about interference. Without clear rules on spectrum sharing and strong regulatory oversight, these conflicts could affect service quality, especially in densely populated urban areas. To succeed, the policy will need careful implementation, including stakeholder consultations and technical safeguards. If done right, this reform could future-proof India's wireless networks and make world-class Wi-Fi access widely available, much like how UPI transformed digital payments in the country.

Official Notification: Use of Low Power and Very Low Power Wireless Access System including Radio Local Area Network in Lower 6 GHz band (Exemption from Licensing Requirement) Rules, 2025

6. INFORMATION TECHNOLOGY SECTOR

6.2 DoT strengthens satellite security regulations amid Starlink and Kuiper's plans to enter India

In May 2025, India's Department of Telecommunications issued strict security guidelines for Global Mobile Personal Communication by Satellite (GMPCS) services, mandating in-country infrastructure, data localisation, and certified equipment to protect national security. While enhancing surveillance capabilities, these rules may increase compliance costs and limit competition by posing high entry barriers for smaller or foreign providers.

Refined Reflections:

In May 2025, the Department of Telecommunications (DoT) released stringent security guidelines for Global Mobile Personal Communication by Satellite (GMPCS) which are services used to provide mobile connectivity via satellite, especially in remote and strategic areas. The new instructions supplement Chapter XII of the Unified License (UL) Agreement and are binding on all licensees authorized to offer GMPCS services in the country. The directions are issued under Clause 39 of Chapter VI of the UL, which empowers the government to intervene in the interest of national security.

The new directives mandate that all gateways and Network Operations Centres be located within India, with interception and monitoring systems approved by Indian authorities. Operators must use only government-authorized VPNs, ensure data localisation, and restrict foreign access to sensitive data. Importantly, user terminals of foreign origin now require certification from Indian security labs, and all equipment must comply with Indian encryption and cybersecurity standards.

While these rules strengthen national security and surveillance capacity especially with global players like Starlink and OneWeb entering the market they could also raise compliance costs, delay service rollout, and could potentially limit competition by imposing infrastructure-heavy requirements such as setting up in-country gateways, certified interception systems, and stringent user terminal approvals, which smaller or newer players may find financially or technically difficult to meet. These obligations could create high entry costs and compliance burdens, potentially deterring international providers or startups from entering the Indian GMPCS market. Additionally, the restrictions on foreign-manufactured equipment and the mandatory use of Indian security certifications may further discourage global participation, ultimately concentrating the market among a few large, well-resourced operators. Going forward, while it's crucial to safeguard national security in satellite communications, it's equally important that such powers are used proportionately and transparently. Security regulations should not become a blanket justification for excessive control or surveillance that stifles innovation or deters investment. Clear checks and balances, stakeholder consultation, and predictable enforcement are essential to ensure that the pursuit of security does not come at the cost of openness, competition, and trust in India's digital ecosystem.

Official Notification: [DoT Issues Stringent Security Guidelines for GMPCS Services](#)