India's Telecom Security Requirements

An indirect trade barrier?

While the objective of the Government to protect national security is legitimate, it should also be mindful that the industry does not suffer because of ad hoc over-regulations, lack of transparency and possible arbitrariness

Vivek Kathpalia, Prerak Hora, Nishith Desai Associates

The Mumbai terror attack of November 2008 has decisively changed India's perspective on its security. The Government is swiftly increasing scrutiny on some sectors of national importance. The telecom sector is one such. Through notifications issued by the Department of Telecommunications (DoT), the Government seeks to regulate the import of equipments or the manufacture of equipments by foreign owned or controlled companies, foreign investment, foreign personnel, access of networks outside India, and information flow outside India.

A February 25, 2010 directive of the Department of Telecom (DoT) requires telecom licensees (unified access, cellular and basic service operators) to furnish the DoT with specific information in order to obtain security clearances for telecom equipment (except passive equipment) and software procured from foreign vendors/manufacturers. According to this directive, however, equipment and software manufactured/developed by Indian owned and controlled manufacturers were exempted from obtaining security clearance.

Another March 18, 2010 DoT directive to unified access, cellular and basic service operators as also to all National Long Distance and International Long Distance operators, Mobile Number Portability licensees, Internet Service Providers (ISPs) pertained to guidelines and clarifications with respect to security clearances as follows :

Security clearance: Required for core equipments per se and not its components.

Technology Transfer by foreign manufacturers: Mandatory inclusion by telecom operators of a clause in their purchase order placed upon foreign manufacturers that such foreign manufacturers must transfer their technology of all critical equipments/software to Indian manufacturers within a period of 3 years from the date of the PO. For any non-compliance of this clause, the vendor/service provider shall be penalized - this could also include criminal penalties.

Minimum or nil dependence on foreign engineers: The operation and maintenance of telecom networks to be entirely by Indian engineers and dependence on foreign engineers to be minimal or almost nil.

Some segments were exempted from security clearance:

Passive equipment and equipment/software manufactured/developed in India by Indian owned/controlled manufacturers.

Hardware/software urgently required for maintenance purposes. However, an intimation to be given to the DoT.

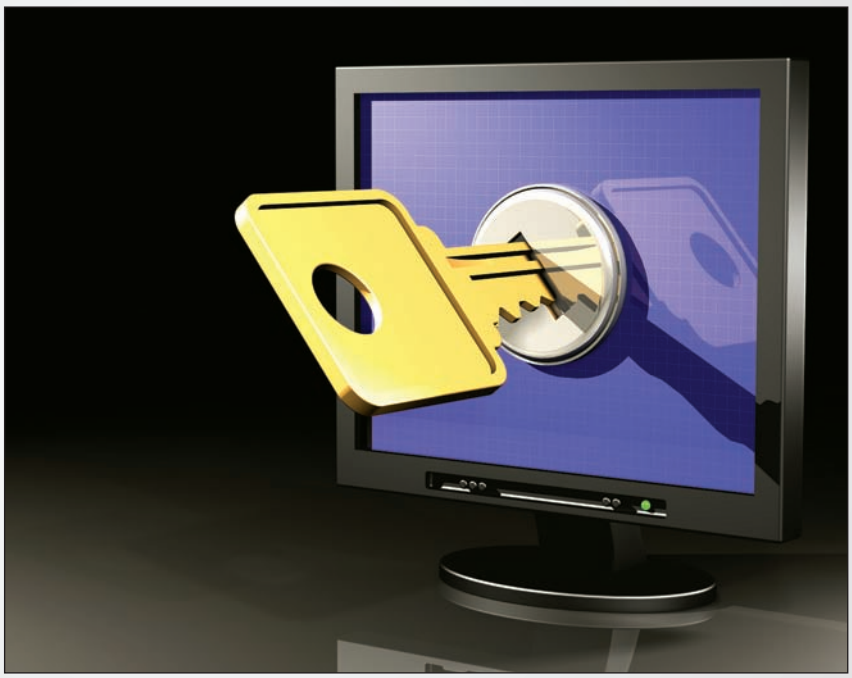
Telecom operators availing pure or managed network services from vendors.

In an attempt to reduce the ambiguity with its earlier directives, the DoT through its July 28, 2010 notification amended the telecom licenses of telecom operators providing basic, unified and cellular mobile services. While this notification provides some clarity on the scope and nature of technology transfer and core equipments, it remains silent on the scope of critical equipment/software. Further, as the notification does not amend the licenses for operators providing services such as NLD, ILD, MNP, ISPs, etc, the ambiguity on the scope of technology transfer, core and critical equipments amongst them, still prevails.

Transfer of Technology against tenets and convention of international law

The intellectual property associated with technology is undoubtedly any vendor's most precious asset. With DoT mandating that foreign vendors part with technology in favor of an Indian manufacturer appears skewing the playing field considering the humungous amount of time and resources that the IP owner would have invested in developing the same.

Apart from the basic argument against transfer of technology, there are a number of other issues that are yet to be addressed. To cite one such – what would the applicable rule be if a foreign vendor acts as a reseller for another foreign vendor? The DoT has also stated that any non-compliance with these provisions would make the licensees and vendors liable for civil and criminal action.



India has, in the past resorted to revoking the Foreign Investment Promotion Board (FIPB) approval granted to a Swiss telecom firm ByCell for offering GSM-based mobile services in India citing security concerns. ByCell then re-approached the FIPB to reconsider its proposal that was quashed subsequently both by the Ministry of Home Affairs that raised concerns over the original sources and channel of flow of funds with respect to ByCell's investment and the Delhi High Court who ByCell had approached for redressal that its licences were withheld despite earlier DoT okays.

In yet another case, for quite some time Canada's Research in Motion ("RIM"), the maker of Blackberry smartphone, has been asked by the Indian security and law enforcement agencies to allow them to snoop into RIM's networks from security perspective as they couldn't access the highly encrypted RIM's networks located in Canada. Blackberry and the Indian security agencies have been having discussions for some time on this issue and recently

RIM has been given an ultimatum by the Indian government to provide encryption details to Indian security and law enforcement agencies for its corporate email and instant messaging services or face a ban on these two widely-used services in India.

Creating ad-hoc regulations that do not provide a level playing field for domestic and foreign players despite being in the nation's highest interests come across as being highly discriminatory. The most appropriate and market-friendly approach would have been for the DoT to address the security concerns in a consultative manner akin to the TRAI consultation paper that was followed by open house discussions with various stakeholders.

While some measures that have been adopted by the government such as security vetting of vendors may be welcome and desirable, the unilateral rights to take over the intellectual property rights of vendors without providing justification has met with widespread disapproval not only from the vendors but from telecom operators. If such measures are not amended, it may result in foreign investors shying away despite the Indian market being so lucrative, otherwise.

Labeling the new stringent security rules as "too tough", business lobbies in the US, Europe and Japan have been putting pressure on India to overturn such strict rules for consistency with global practices and also as their feedback was not sought during the formulation of the policy. The DoT has been requested by the Prime Minister's Office to examine the rules in consultation with the MHA and in light of international best practices. . Whether imposition of such conditions would constitute a violation of the World Trade Organisation's principles by qualifying as a non-tariff barrier also remains to be seen.

In conclusion while the objective of the Government to protect national security is legitimate, the Government needs to be mindful that the industry does not suffer because of ad hoc over-regulation, lack of transparency and possible arbitrariness. It could leave the scope open to abuse and corruption. The earlier the Government takes cognizance of these issues, the better.

Minimum or nil dependence on foreign engineers: The operation and maintenance of telecom networks to be entirely by Indian engineers and dependence on foreign engineers to be minimal or almost nil.