Encryption and contradictions of the regulations in India

The Indian Government's recent efforts to regulate 'Voice-over-Internet Protocol' providers and insist that they set up servers in India to enable monitoring and real time access to data feeds (voice and non-voice) by the national security agencies is uncannily following a very similar to that adopted with respect to BlackBerry's manufacturer, Research In Motion (RIM) Limited, a few years ago, in relation to the use of 256-bit encryption. A part of the current problem emanates from the continued inability of the Indian security establishment to intercept secure communications using high-level encryption, which is the case with many VoIP operators. To add to the quandary, a continuously conflicting set of Indian telecommunications regulations and other laws pertaining to the use of high-level encryption are currently in place in India.

Internationally there has been a movement towards governments prescribing only the minimum level of encryption and permitting use of high-level encryption for secure private communication by corporates and individuals. In India however, even after prolonged lobbying from e-commerce and IT industry bodies and amendments to the Information Technology Act 2000, the regulations pertaining to the use of encryption technologies are still a legal quagmire and the sector is desperately in need of a clear, national encryption policy.

Sector-specific regulations

India does not have any encryption policy nor is there specific legislation governing the use of encryption techniques to secure electronic communication. The basic legislation concerning electronic data and communication and its processing, the Information Technology Act, 2000 (IT Act) is also silent on the level and type of encryption that a person or organisation can deploy to protect electronic communication and data.

The government's Department of Telecommunications (DoT) in the 'Guidelines for the grant of Licence for Operating Internet Service' (ISP Guidelines) and in the 'Licence Agreement for the Provision of Internet Service' (ISP Licence Agreement) that is entered into between the DoT and the Internet Service Provider (ISP) for the provision of internet services in India has laid down that the individuals and corporates while using the ISP services are permitted:

"*to use up to 40-bit key length in the symmetric key algorithms or its equivalent in other algorithms without having to obtain permission from the DoT, but for use of any encryption equipment higher than this limit, the same can be done only with the prior approval of the DoT".*

In addition to the ISP Guidelines and the ISP Licence Agreement, there are various sectoral or industry-specific regulations already in place in India that prescribe a higher level of encryption of more than 40 bits:

<u>Securities and Exchange Board of India Guidelines on Internet Based Trading and Services</u>

The Securities and Exchange Board of India (SEBI) prescribes a 64-bit/128-bit encryption for standard network security and mandates the use of encryption

technology for security, reliability and confidentiality of data. SEBI recommends use of secured socket layer security preferably with 128-bit encryption, for securities trading over a mobile phone or a wireless application platform.

Reserve Bank of India Guidelines on Internet Banking

The Reserve Bank of India (RBI) has recommended public key infrastructure, as the most-favoured technology for secure internet banking services, as per its guidelines issued on internet banking of June 2001.

In view of the limited availability, it was recommended that, for secure internet banking transactions, the banks should use at least 128-bit encryption secured socket layer for securing the browser to web server communications and encryption of sensitive data such as passwords in transit within the enterprise itself.

The Information Technology (Certifying Authorities) Rules, 2000:

The Government of India under the Information Technology (Certifying Authorities) Rules, 2000, issued by the DoT, has laid down the IT Security Guidelines for implementation and management of IT security. These rules state that electronic communication systems used for the transmission of sensitive information, such as routers, switches, network devices and computers, must be equipped with suitable security software and, if necessary, with an encryption software. The Rules also provide that stored passwords must be encrypted using 'internationally proven encryption techniques' to prevent unauthorised disclosure and modification. Such 'internationally proven encryption techniques' require RSA public key technology standards such as PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit), PKCS#5 Password Based Encryption Standard or PKCS#7 Cryptographic Message Syntax Standard as mentioned under Rule 6 of these rules. The encryption algorithms provided by these rules are very strong and secure.

Data Security Council of India views:

With regard to the amendments to the IT Act, the DoT sought views of the Data Security Council of India (DSCI) on Encryption Policy. The DSCI in its recommendations of 13 July 2009 recommended adoption and implementation of an Encryption Policy and suggested that:

"Use of symmetric encryption for e-commerce applications, including SSL for end-to-end authentication, be allowed with encryption of up to and including 256 bits with AES algorithms, or equivalent algorithms."

Despite the above recommendation, no provisions for the use of high-level encryption were introduced by the Government in the amendments to the IT Act or the encryption policy enacted by the Government.

Conflicting set of regulatory obligations

The maximum 40-bit encryption level provided for under the ISP Licence Agreement as per the DOT's present licensing regime perpetuates an outdated and technologically obsolete approach. This leads to a growing difference between DoT regulations and sector specific legislations enacted by the Government of India.

Both the national long distance and international long distance licences make it mandatory for the service provider to have prior evaluation and approval from the Department of Telecommunications or an officer specially designated for the purpose, before connecting and installing any encryption equipment to its network. The ILD licence also prevents such service providers from employing 'bulk encryption' equipment in their network.

Finally, the ISP Licence Agreement also restrains ISPs from deploying 'bulk encryption' and restricts the level of encryption for individuals, groups or organisations to a key length of only 40-bits in symmetric key algorithms or equivalents. Such levels of encryption are very weak and can be easily broken and by-passed and are not suitable for e-commerce or any other sensitive applications.

In cases where the entities want to use more than 40-bit encryption, they need to obtain specific approval from the DoT with regard to such usage.

It is clear that there exist stark discrepancies between the levels of encryption recommended under the various sector-specific legislative enactments and the Department of Telecommunications licensing regime.

Use of higher levels of encryption and the regulatory requirements

As is stated in the ISP Licence Agreement, the use of encryption of more than 40 bits requires the prior approval of the DoT and the deposit of the decryption key in two parts, when required.

In order to be able to use encryption of more than 40 bits, such persons or organisations are needed to comply with certain further obligations and conditions laid down with regard to the same as per the ISP licence. These obligations have been briefly encapsulated below:

Inspection and testing of installations

The DoT or the Telecom Regulatory Authority of India (TRAI) may require certain tests to be carried out for the installations deployed. There may also be a requirement to supply the DoT or TRAI with all the necessary literature and drawings, etc, for the equipment installed.

Right of DoT to inspect

DoT has the right to inspect the sites used for the provision of higher levels of encryption, including access to all necessary facilities for the provision of the same.

Prohibited activities

The DoT imposes a duty on such person or organisation using more than 40-bit encryption not to undertake certain activities in light of security concerns and a duty to be in compliance with the laws of India with regard to the content.

Security conditions

Certain security conditions have been prescribed by the DoT, which are to be complied with by the person or organisation using more than 40-bit encryption. These are with

regard to the mode and manner of services and the details of filings to be made with the various Indian authorities at different points in time.

Monitoring facilities

The person or organisation using more than 40-bit encryption would be required to comply with some requirements for monitoring. These relate to the office space to be used and the equipment to be deployed.

In the absence of any clear and specific law and the existing conflicting sector-specific regulations, the ISPs and the only option the consumers are left with is to approach the DoT to seek approval to use more than 40-bit encryption. There is no procedure laid down for obtaining the said approval of the DoT and also the procedure, guidelines and criteria that the DoT has to adopt to approve the proposal to use more than 40-bit encryption. It is clear that there remain stark discrepancies between the level of encryption recommended under the IT Rules, SEBI Guidelines and RBI internet banking guidelines on the one hand, and the Department of Telecommunications Licensing Regime relating to the ISPs, NLDs and ILDs on the other.

However, despite the furore around the Blackberry issue in the past and subsequent amendments of the Indian Information Technology Act, the Government has yet to clarify the situation of contradictory regulatory requirements as laid down by its own departments and institutions, to implement a clear policy for use of high-level encryption for secure private communication, and to provide a clear procedure for obtaining any permissions required for the same.