scriboard®
Advocates & Legal Consultants

the
IP-TECH
law series
2018

Guide to

Indian Law on Encryption

LAW WIRE®
COMMUNICATING THE LAW™

Indian Law on Encryption

Under Indian Law Section 84A of the Information Technology (Amendment) Act, 2008 empowers the government to prescribe the modes or methods of encryption "for secure use of the electronic medium and for promotion of e-governance and e-commerce". But the rules have not been notified so far although draft recommendations have been made available.

As a general practice 40 bit encryption equipment has been used in India with a more advanced encryption system for sensitive information. Although, there are a few exceptions like SEBI and RBI which have prescribed industry specific but different encryption standard ranging from 64 bit to 128 bit. As for the Department of Telecommunications, the National and International Long Distance License Agreements (NLD and ILD) demands prior approval of Department of Telecommunications pertaining to installation of encryption equipment whereas the Internet Service Provider (ISP) license agreements specifically bars encryption strength of over 40 bits.

Moreover, the restriction pertaining to 40 bits encryption [and proposed to be 128 bits] is a generally applicable rule. In case where the encryption equipment uses more than 40 bits, the equipment needs to be approved by the Government of India and in particular cases, the Government asks for the decryption key. Presently, the Government of India has the infrastructure to monitor networks that employ 40 bits encryption and need not be provided with a decryption key in such cases. The main concern is the proprietary nature of the encryption code. The companies do not wish to provide decryption key for their proprietary software and open a backdoor for the Government which also compromises privacy.

Please note that there is no uniformity amongst various Government Departments and Regulatory authorities. DoT permitted encryption standards are not uniform with the standards prescribed by other regulatory bodies as also they are inconsistent with the International Standards.

Contentions / Issues

1. Standard encryption limits not known
2. 40 bit Encryption standard is outdated
3. 40 bit encryption can be easily hacked by a Brute Force Attack
4. Whether 256 bit encryption standard should be applied or not?
5. Proprietary encryption software

Industry specific general practices

Businesses and communications companies need encryption to protect their information from being compromised as the use of encryption is not limited to Government authorities. Please find below general practices followed by various regulators pertaining to encryption:

A. Securities and Exchange Board of India [SEBI]

1. Mandates the use of Encryption
2. Prescribes 64 bit/128 bit encryption for network security

3. Recommends 128 bit encryption for both WAP based securities trading and internet based securities trading.

B. Reserve Bank of India [RBI]

1. Mandates the use of Encryption for banks
2. Makes the use of SSL/128 bit encryption as minimum level of security
3. Strong Encryption to be used for protection of sensitive and confidential information of bank and customers in transit

C. Department of Telecommunications [DoT]

1. NLD License
   - Mandates evaluation and approval of Encryption Equipment
   - Makes the Licensee responsible for protection of privacy of communication
2. ILD License
   - No Bulk Encryption
   - Mandates evaluation and approval of Encryption Equipment
3. ISP License
   - No Bulk Encryption
   - Level of Encryption limited by DOT to 40 bit key length
   - For use of encryption more than the prescribed limit of 40 bit, written permission of DoT required with mandatory deposit of the Decryption Key with DoT

D. The Information Technology (Certifying Authorities) Rules, 2000

- 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
- Stored passwords must be encrypted using 'internationally proven encryption techniques' to prevent unauthorised disclosure and modification
- '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

E. Indian Railways [Online Ticketing]

- Credit card information should be fully encrypted (128 bit, browser independent encryption)
- To ensure security card details are NOT stored

Regulatory requirements for encryption higher than 40 bits

1. Approval of the DoT
2. Depositing decryption key with DoT
3. Inspection of encryption equipment / installations
4. Testing of encryption equipment / installations
5. Mandatory prohibition of certain activities in the light of national security
6. Registering with / Informing certain Security Agencies / Indian Authorities
7. Interception, Monitoring and Decryption facilities

Encryption Policy [Draft] under Section 84A

The Data Security Council of India [DSCI] along with NASSCOM has recommended 128 bit encryption standard as apposed to the previously prescribed standard of 40 bit. Legitimizing 128 bit / 256 bit encryption has been well perceived amongst all industries as well as the government. As we understand the present situation, there has been no formal communication of the decision of the Government to enhance encryption standard to 128 bit / 256 bit.

Discussions / Observations under the draft rules:

The scenarios that require use of encryption in e-commerce applications that may be covered by an Encryption Policy under Section 84A broadly fall in two categories namely, Data at Rest, and Data in Transit. Various scenarios in these two categories are as follows:

1. Data at Rest: Corporate data stored in data servers, end points that include Desktops, Laptops, Personal Digital Assistants (PDAs), Mobile Phones with e-mail, USB Drives, Backup tapes and other media- all of these contain corporate data that can be encrypted if required by data protection considerations. It should be noted, however, that mobile devices are not always capable of encrypting data at rest due to functionality limitations of the equipment these may use other mechanisms to protect stored data such as passwords to unlock a device. In fact, more and more clients are demanding that their Data at Rest be protected through some mechanism from password to encryption.
2. Data in Transit: Corporates are communicating with their clients, trading partners, collaborators and their service providers which typically include exchange of document including RFPs, proposals, commercial quotes, deliverables, operational e-mails and other types of sensitive data among designated individuals. Encryption is often employed to protect these types of Data in Transit, although there may be scenarios where the underlying document may be encrypted but the communication may not require encryption.

Even more complex may be the management of keys for SSL / TLS sessions. Those keys are generated randomly and only used for a particular session – for a variable period of time (for example the length of a e-commerce purchase on a website) Managing keys for this use scenario quickly grows exceedingly complex, and in fact may be entirely useless when the data at either end of the encrypted SSL / TLS reverts back to the original plain text otherwise the customer would not be able to see the web catalog, or the vendor would be unable to process their payment for lack of account information. Put simply, there may be more efficient ways to obtain the clear text than trying to decrypt the data in transit.

Monitoring at the gateways in real-time:

All mails, documents, and transactions must take place pass through Internet/communication gateways of the country. If these are to be monitored, which we believe must be for specific persons, for specified time durations, through a court order or a due process that is transparent, then LEA may need access to keys for decrypting the communications in real-time. It is difficult to visualize the need for LEA to intercept all traffic from a company in real time. It is presumed that such a step, if absolutely essential, will be resorted to with due process, for specific IP addresses

only. Providing plain text data to LEA without resorting to key recovery is the right approach.

Data Security Council of India [DSCI] recommendations:

1. Use of symmetric encryption for e-commerce applications, including SSL for end-to-end authentication, is allowed with encryption of up to and including 256 bits with AES algorithms, or equivalent algorithms.
2. LEA may be provided with plain text of encrypted communications that it wants to monitor, within a reasonable time of request being made, only after a due process has been followed, that is transparent and subject to oversight.
3. Plain Text Disclosures - Corporates may cooperate with the government and LEA by providing plain text information, within three business days of a request being made. This will include making available information from both Data at Rest as well as Data in Transit. Where possible, companies will expedite such disclosures where LEA indicates greater urgency in the request.
4. Difficulties of Implementation
5. It is important for the government to note that corporates providing services to their clients abroad have signed what is known as Master Service Agreements (MSAs). Even providing of plain text information to LEA will have a bearing on MSAs signed with customers and partners.
6. Change in existing technology/devices would attract capital investment, and a long lead time to implement.
7. It is also observed that centralized encryption platforms are very expensive and require skilled resources; majority of companies will find it difficult to implement.
8. Proprietary Encryption - Some software like Skype use proprietary encryption which will not be disclosed. Several outsourcing companies use such software for communication. How will the government verify and approve proprietary algorithms? Instead of mandating approved algorithms, it should ‘recommend’ their use. This 'recommendation' of algorithms does not affect the security posture since the amendment requires that companies must provide plain text information when requested by LEA.

SCRIBOARD
Advocates and Legal Consultants

www.scriboard.com

Scriboard is a full-service commercial law firm with cutting-edge specialisation in intellectual property, commercial laws, domain name disputes, data privacy / protection, technology including compliance, new media, telecommunications, legal training and allied services. Scriboard regularly advises Fortune 500 and other leading multinational and national companies on a plethora of issues.

LAWWIRE
Communicating The Law

www.lawinfowire.com

Law Wire is a platform, which focuses on providing an in depth coverage on the ever changing Intellectual Property, TMT and New Media Law sector in India and the world. Law Wire bridges the gap between legal knowledge on one hand and the legal policy making on the other. Law Wire is also a platform where readers would get an in depth knowledge of issues pertaining to Intellectual Property and Information Technology Law. This platform endeavours to provide an opportunity to lawyers [including law students] and other professionals in the legal domain to express their views and work in a collective capacity.