INTRODUCTION

The legal position with regard to encryption technology has always been somewhat ambiguous. There is a provision in the ISP regulations that individuals/groups, etc. should not use encryption higher than 40 key bit length unless they deposit the keys of the same with the government. It has never been clarified whether this refers to only the ISP’s or to their customers also. ISP’s and other Telco’s are in any case subject to detailed regulations on use of encryption, providing the government with access to their systems, etc.

Businesses in India have gone about implementing much higher levels of encryption. In fact, regulations relating to online securities trading and online banking itself prescribe higher levels of encryption.

In the recent past, there have been some rumours about the government coming out with regulation in this area, though the focus has been more on data localization. Ever since the reference to data localization was made in a draft M2M roadmap document, there has been silence from the government on the issue.

On September 19, 2015, the Government issued a paper called the National Encryption Policy. Within a couple of days of its release, the paper drew sharp criticism, not to mention derision at the proposals contained in the policy. On September 22, 2015, the government clarified that the requirements of the policy would not apply to mass used applications such as Whatsapp, Facebook, etc. Later in the day, the concerned Minister announced that the policy has been withdrawn and stated that it would be redrawn to specify clearly to whom the requirements of the policy applies.

We have provided below, a summary of the key provisions of the policy.

SUMMARY OF THE NATIONAL ENCRYPTION POLICY

The policy sets out its applicability to different groups. By and large, there is the government (G), businesses (B) and consumers (C). The language used for B2B, B2C and C2C transactions is more or less the same. By and large, there are three requirements:

1. Encryption algorithms and key sizes will be prescribed by the Government through notifications from time to time. (This could mean minimum standards but more likely, it will involve maximum level of encryption permitted)

2. On demand, the user should be able to reproduce the same plain text and encrypted text pairs using the software / hardware used to produce the encrypted text from the given plain text.

3. Such plain text information has to be stored by the user/organisation/agency for 90 days from the date of transaction and made available to law enforcement agencies as and when demanded in line with the provisions of the laws of the country.

The second point above does not seem to apply to C2C communications.

The policy also provides that service providers located within and outside India using encryption technology for providing any type of services must enter into an agreement with the Government for providing such services in India. Users in the G, B and C categories taking services from these service providers are responsible for providing information in plain text format when demanded.

ANALYSIS

The policy can be criticized on many grounds. To start with, the government should not be prescribing encryption levels (especially maximum levels). It is acceptable to specify minimum levels in specific industries such as telecom, banking, etc but the language of the policy appears to be far broader than that. Further, there is a concern that if you wanted to use a higher level of encryption than what is prescribed, you would have to deposit the keys with the government.
The requirement to keep content in plain text form for 90 days is outright ridiculous. The government is already prescribing that if it wants the information, you have to provide it. If so, why insist on keeping it in plain text form? Doing so means the information that you want to encrypt would not be encrypted and therefore not protected. It seems to be an absurd approach.

The reference to service providers providing services within or outside India is quite ominous. Every offshore operation in India, every BPO entity at the very least, but very likely, most sophisticated companies will be using encryption technology to provide services. It is not known what the agreement which they have to sign will say. Again, the concern is that it will state that if one wants to use encryption above a particular level, one has to deposit of keys with the government.

Overall, it is not surprising that following the uproar in the online community over the policy, it was withdrawn by the government. It does speak very poorly about the competence of those engaging in policy making at the Ministry of IT. For now, the policy stands withdrawn but it leaves a sense of uncertainty as to what would be the regime concerning use of encryption in the future. We advise clients to continue to use encryption technology in India as they wish. We believe that industry will talk to the government and convey the need for a far less restrictive policy.

ABOUT KOCHHAR & CO

Kochhar & Co is a leading full service commercial law firm with the best national presence among all law firms in India. The firm mostly represents international companies doing business in India and offers a high quality, business oriented service to its clients. The firm takes great pride in its client servicing approach which is focused on clarity, accessibility and providing business solutions. The firm has the largest national presence in India with offices at Delhi, Gurgaon, Mumbai, Bangalore, Chennai and Hyderabad.

TECHNOLOGY LAW PRACTICE

Kochhar & Co set up India's first Technology Law Practice, which has been the leading tech practice in the country ever since. The practice covers areas such as licensing, outsourcing, e-commerce, telecom, intellectual property, regulation of STP's and SEZ's, social media, etc. The firm has the largest clientele of international technology companies doing business in India. Chambers rates Kochhar & Co as a Tier 1 law firm in India for TMT work.

CONTACT DETAILS

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stephen Mathias</td>
<td><a href="mailto:stephen.mathias@bgl.kochhar.com">stephen.mathias@bgl.kochhar.com</a></td>
</tr>
<tr>
<td>Suhas Srinivasiah</td>
<td><a href="mailto:suhas.srinivasiah@bgl.kochhar.com">suhas.srinivasiah@bgl.kochhar.com</a></td>
</tr>
<tr>
<td>Rianna Lobo</td>
<td><a href="mailto:rianna.lobo@bgl.kochhar.com">rianna.lobo@bgl.kochhar.com</a></td>
</tr>
<tr>
<td>Naqeeb Ahmed Kazia</td>
<td><a href="mailto:nageeb.ahmed@bgl.kochhar.com">nageeb.ahmed@bgl.kochhar.com</a></td>
</tr>
</tbody>
</table>