**ABTO/ 54/ 2004/ 051** **15th March 2004**

Shri Pradip Baijal,
Chairperson,
Telecom Regulatory Authority of India,
A2/14, Safdarjung Enclave,
Opp. Bhikaji Cama Place,
New Delhi – 110 029.

**Sub: ABTO Response to TRAI's Preliminary Consultation Paper No. 2/2004 on Mobile Phone Theft**

Dear Sir,

Please find enclosed ABTO response to **TRAI's Preliminary Consultation Paper No. 2/2004 dated 8th January 2004 on Mobile Theft.**

ABTO shall be grateful, if our suggestions contained in the Annex is considered by TRAI while making its recommendations.

Thanking you,

Yours faithfully,

**(S.C.KHANNA)**
**SECRETARY GENERAL**

CC : Dr. D P S Seth, Member, TRAI
Mr.P.K. Sarma, Member, TRAI
Dr. Arvind Virmani, Member, TRAI (Part Time)
Prof . Sanjay Govind Dhande, Member, TRAI (Part Time)
Dr Harsha Vardhana Singh, Secretary cum Principal Advisor, TRAI
Mr. M. Kannan, Advisor (Econ), TRAI
Mr. R K Bhatnagar, Advisor (FN), TRAI
Mr. Rajendra Singh, Advisor (MN), TRAI

**ANNEX**

# ABTO Response to TRAI's Preliminary Consultation Paper No. 2/2004 on Mobile Phone Theft

## Introduction

ABTO believes that in India like in other countries, a mechanism should be put in place where mobile phone theft can be curbed. Presently, in our country there are over 30 million mobile subscribers and in the next two years we expect that this number would swell to reach about 100 million users. With the growing importance of mobile phones in daily lives of the common man, and the increasing new wave of applications which are expected to be introduced on mobile phones such as m-commerce –mobile phone theft could come as a serious roadblock in the growth of these advanced day-to-day applications. This will jeopardize the investments and valued efforts of service providers and content developers since the mobile users would be apprehensive to avail these services because of the lurking fear of his mobile phone getting lost / stolen and being misused leading to all kinds of disputes. It is therefore appropriate and absolutely necessary that the industry – manufacturers and service providers along with the Government – the Regulator and law enforcement agencies come forward and put in place a fool proof mechanism which can help curb the menace of mobile phone theft.

ABTO appreciates the TRAI's effort to float a preliminary Consultation Paper to sensitize the thought process of stakeholders so that through this methodology, a detailed analysis could be made on the international practices so that the Indian consumer's interest is protected. It is imperative that the Authority carry out an independent analysis to assess the magnitude of the problem in the Indian context.

While ABTO supports the initiative taken by TRAI, it must be cautioned that the entire process must be simple to implement from the perspective of all i.e. the customer, service provider, manufacturer and law enforcement agencies so that there is an incentive to all stakeholders to embrace the same. Another important aspect would be that of costs and it must be seen that the Regulations do not put additional burden through exorbitant costs on service providers for implementation of the same as this will then work at cross purposes of providing affordable services. ABTO thus suggests that the Regulation must have minimal cost implication on service providers.

TRAI's preliminary Consultation Paper covers the aspects regarding mobile phone theft of GSM phones mainly. This problem is somewhat different in the case of CDMA mobile phones. Since the growth in CDMA mobile phones is explosive with over 6.5 million subscribers today, security from mobile phone theft is a matter of concern for these users. There is very little data that is available on the CDMA side. TRAI would be in a better position to pool in these resources from other countries where CDMA networks are deployed.

To summarise the above, the methodology for implementation in India, the following need to be analysed in greater detail and would need to be transparently discussed before finalization of the regulations:

- IMEI and CEIR are relevant to GSM mobile phones only. What happens in the case of CDMA where there is no IMEI?
- Centralised database for CDMA mobile phones is not known.
- Anti-theft measures adopted should be fool-proof.
- Procedures should be easy to implement.
- What would be the cost implication on service providers?

We have attempted to put forward some suggestions to focus our reply which is dealt with in the subsequent paragraphs which may be appropriately considered by TRAI.

## Security Issues in CDMA mobile phones

CDMA phones do not have a SIM card and it is the phone itself that is connected directly to the network. The electronic serial number (ESN) is a unique identification number embedded or inscribed on the microchip in a CDMA phone by the manufacturer. The ESN is used in generating CDMA encryption keys. It is distinct from the Mobile Identification Number (MIN), which is the service providers' identifier for a phone in the network.

The most critical issue with respect to security of CDMA mobile phones relates to the hacking of software for cloning or reprogramming are:

I) ESN cloning within the same network –

Unscrupulous elements obtain valid ESN/MIN combinations illegally from the CDMA mobile phones of legitimate subscribers. This ESN/MIN combination is then replicated onto an illegitimate mobile phone whose user can make calls at the cost of the original ESN subscribers.

II) Hacking for activation on another network –

Each CDMA mobile phone is supposed to have a unique factory configured ESN, which is then activated to exclusively work within the network on which it is provisioned for. Through hacking of the software in the phone these configurations are changed and the phone can be activated on the network other than the one it is provisioned for.

This cloning and hacking of software through illegal reprogramming of mobile phones needs to be eradicated. This issue can be tackled on three fronts:

### 1) Technical

2) **Consumer awareness**
3) **Legislation**

## 1) Technical Solutions

Solutions need to be primarily devised on the technical front to make the security of the phones full proof. Both the manufacturer as well as the service provider needs to be actively involved in this initiative.

**A) Manufacturers**

1) Manufacturers should be asked to continuously increase the level of security in the handsets and they should come with cost effective standards.
2) Manufacturers should be forced to take all technical measures possible to prevent the hacking of software and cloning of ESN.

**B) Service Providers**

1) The service providers shall bar the activation of ESN numbers provisioned on other operators network. This issue can be approached as:

    a) All service providers shall maintain individual databases to store the ESN numbers of the handsets used by subscribers activated on their networks.
    b) Preparation and updation of such a database shall be the responsibility of the individual service provider.
    c) These databases can be shared across operators to form a central registry/database.
    d) The central database may be managed through an industry association.
    e) ESN's of only those handsets which have been legally imported / sold shall form a part of this database.
    f) When a range of ESN's is allocated to a service provider, then it should be linked to the respective service provider.
    g) Only when the service provider releases a particular ESN from the link, it can be moved to the next zone of 'free for activation'.
    h) Before processing any request for provisioning of a handset on a network, (where ESN is not already allocated to the service provider,) the concerned service provider must verify whether the number is in the zone – 'free for activation' and only then it should be provisioned on its network.

## 2) Consumer awareness

i) Create public awareness about the offence.

ii) Service providers need to offer security advice prominently on their websites and manufacturers need to give greater prominence to security message in their manuals.

iii) A campaign to better advise consumers of the practical steps they need to take to reduce the risk of becoming a victim of mobile theft such as improved information on handset security features, an advertising campaign, etc

iv) Encourage immediate reporting of stolen phones in view of scope of barring the handset across all networks.

## 3) Legislation

i) Introduce legislation and stringent penalties or enabling the law enforcement agencies to take action against those indulging in the following violations by declaring it illegal:

- For rewriting or changing the software of the mobile phone
- For reprogramming the handset
- For cloning the handset
- For introducing extra hardware or software to change the identity
- For possession, use, manufacture or sale of hardware or software used in cloning or hacking.

ii) Making it illegal to specifically own or use a stolen mobile phone.

iii) Taking strict action against import/export of stolen mobile phones. Most of such grey market handsets find their way into the country at the cost of National Exchequer by evading customs duties.

In UK, under the 'Mobile Telephones (Reprogramming) Act 2002', a person guilty of any of the above offence made liable to imprisonment for a term of minimum 5 years and a fine not exceeding the statutory minimum.

Thus, a complete preventive system needs to be put in place with an overall aim of removing the reward to phone hackers and thieves by making stolen and reprogrammed phones impossible to use.

**********