RCOM Response to the TRAI Consultation Paper on "Issues relating to Blocking of IMEI for Lost/Stolen Mobile Handsets"

General

1) We support TRAI's proposal that a mechanism should be put in place where mobile phone theft can be curbed. In our country there are over 675 million mobile subscribers and with the growing importance and affordability of mobile phones in daily lives of the common man the figure is about to touch 750 million within this financial year. With increasing subscriber base loss of a mobile phone is emerging as a serious concern to the consumers not only because of cost of handset but also valuable personal data stored in it in the form of photos, contact list and other important information is lost. In future, the level of security of the phones will become increasingly important when these phones will also be used as financial transaction terminals.

2) It is 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.

3) We congratulate the Authority for coming up with a customer friendly issue. Today, in case of theft or loss of a mobile phone, the service providers are providing the facility of blocking the SIM card but there is no mechanism in place to block a lost mobile phone.

4) The Authority has discussed other modes of addressing the mobile thefts also i.e mobile tracker. It is also felt that mobile insurance can also be one mode, wherein a subscriber can insure his/her handset. This option can be considered in case of costly handset, specially when 3G networks will be launched by many operators, and the handsets supporting 3G network will be costlier. However, the penetration of insurance products may take some time in our country.

Issues concerning CDMA Devices

5) While we support the TRAI initiative but it must be cautioned that the consultation Paper generally covers the mobile phone theft for GSM phones and does not specifically address issues relating to the CDMA phones. Since the growth in CDMA mobile phones is substantive with around 125 million subscribers today, security from mobile phone theft and loss is also a matter of concern for these users.

6) International Mobile Equipment Identity (IMEI) is a unique serial number which identifies the GSM handset. A subscriber identification module (SIM) on a removable SIM card stores unique the service-subscriber key (IMSI) to identify a subscriber. Thus there are separate IMEI and IMSI on GSM devices and both are separately transmitted over the air.

7) ESN is a unique serial number which is given to CDMA devices. Unlike in GSM where all devices are SIM based, there are two types of CDMA handsets namely Non Removable User Identity Module (Non-RUIM) and Removable User Identity Module (RUIM). In Non-RUIM handsets each time a call is placed, the ESN is automatically transmitted to the base station so the wireless carrier's mobile switching office can check the call's validity. Therefore in Non-RUM based handsets, unique ESN is transmitted. However, in RUIM based handsets UIMID (user identity module identifier) is in a R-UIM . In all known systems, the UIMID displaces the ESN in signaling and therefore RUIM based handsets cannot be tracked using ESN. Since UIMID is placed on RUIM and not on the handset, tracking /blocking a stolen/lost CDMA handset will not be possible.

8) Therefore IMEI and CEIR are relevant to GSM mobile phones only and will not address the issue for CDMA phones.

Issues Concerning GSM Devices

9) Unlike the ESN of CDMA, the IMEI is used only for identifying the device and has no permanent or semi-permanent relation to the subscriber. Therefore blocking of stolen/lost GSM handsets using IMEI is possible. However, there is serious limitation with regard to using IMEI number for blocking or tracking stolen or lost handsets as new IMEIs can be programmed into stolen handsets.

10) In rapidly growing mobile market, there are million of subscribers who are using handsets with reprogrammed IMEI numbers. With such a large number of duplicate IMEIs being used, blocking a handset with duplicate IMEIs would cause serious consumer discontent as all the other handsets with the same IMEI will also be blocked.

11) Therefore it may be desirable to first assess the extent of the problem that is caused by reprogrammed IMEI numbers before putting in place a suitable mechanism to address the same. In UK, Mobile Telephones (Reprogramming) Act, 2002 has been promulgated to declare tampering of IMEI number as illegal. Even these laws have not helped much as reprogramming is generally undertaken out of sight, in the back rooms of premises, and it is therefore difficult to prove that reprogramming is carried out.

12) To summarise the above, the following needs to be analysed and would need to be transparently discussed before finalization of the regulations:

- IMEI and CEIR are relevant to GSM mobile phones only.
- ESN is unique number given to CDMA devices but in RUIM based phones UIMID replaces ESN in signaling. Since UIMID is placed on RUIM and not on the handset, tracking/blocking CDMA handset on the basis of UIMID is not possible.
- There are millions of GSM devices with duplicate IMEIs. The process cannot be implemented unless one time cleaning up is carried out.

Our point wise response follows:

1) **In order to reduce/discourage mobile theft do you think the blocking of IMEI is an effective solution? Please give reasons.**

The blocking of IMEI number can be an effective solution to discourage GSM handset theft. However, there are following two major challenges which may make it difficult to curb theft using IMEI based solution alone:

- There are millions of GSM handsets available in the market with duplicate IMEI numbers. As per the statistics available, around 10 % of current IMEIs in use may be reprogrammed. Genuine users will lose their service in case IMEI blocking request comes from tampered handset user. **To make this process robust the duplicate IMEIs will have to be phased out, in the one time clean up exercise.**

- **In CDMA handsets ESN is a unique serial number corresponding to IMEI for GSM handsets. In the Non-RUIM handsets each time a call is placed, the ESN is automatically transmitted to the base station so the wireless carrier's mobile switching office can check the call's validity However, in RUIM based handsets UIMID (user identity module identifier) is in a R-UIM which displaces the ESN in signaling. Therefore RUIM based handsets cannot be tracked/blocked using ESN.**

2) **In case blocking of IMEI is implemented, to what extent load on the network will increase? Please give details**

At this juncture, it is felt that there may not be increase in load on the network. However, as the list of blocked IMEI number increases with passage of time, the load on network will go up. We hope that the Authority will come up with rules regarding retention period for the blocking of IMEI number. **The retention period should not be more than six months or year at the most.**

3) **In your opinion who should maintain the CEIR? Please give Reasons.**

A third party- just like NDNC for DNC registry can be considered for maintaining the Centralised Equipment Identity Register. NIC has gained sufficient experience for maintaining large databases and sharing that on real time basis with telemarketers and service providers. The NIC will also be maintaining more complex database based on consumer preference for Do Not Call registry. Therefore NIC is most suited to maintain CEIR.

4) **Should the CEIR be maintained at national level or zonal level? Provide details including the estimated data size.**

The CEIR should be maintained at National level. Even national database are ineffective as stolen handsets find their way across international boundaries. Therefore the national CEIR should be integrated with the global CEIR. This would mean that once a customer has reported his/her phone as stolen or lost to his/her network operator, the phone would be blocked from many countries across the Globe. This would significantly reduce the incentive for stealing mobile phones.

Considering the mobile subscriber base is around 700 million a theft/lost rate of 1%, about 10 million capacity should be considered initially. However, there should be enough capacity in the system to meet the burgeoning requirement of the subscriber base.

5) **Please comment on cost and funding aspects of Centralized EIR? Please provide detailed cost estimates?**

EIR feature is required to be implemented in the switch. A highly stabalised link is required between MSCs and common EIR. In the event of the link failure IMEI blocking may be affected. A very high grade EIR hardware/software is also required so that it can cater to all cellular subscribers in India.

At first Capex will be required to set up centralized EIR data base. The EIR will have to be connected on real time basis to MSCs. Subsequently OPEX will be required for updating and maintaining data base. The task of implementing the project can be given to DIT / NIC.

The funding of the CEIR in terms of CAPEX and OPEX can be from TRAI consumer education fund or from the government on the lines NDN registry is setup and maintained.

6) **Should blocking of IMEI /ESN be chargeable from customer? If yes, what should be the charge?**

A nominal charge should be allowed to the service provider for blocking of handset. This will cover the expenses on administration, customer care and creation of hardware and software to run the blocking of IMEI process.

7) **Please give your views on bringing a legislation to prevent reprogramming of mobile devices? In your opinion what are the aspects that need to be covered under such legislation?**

The purpose of blocking of IMEI number stands defeated in case handset is re-programmed and duplicate IMEI is implanted on the stolen/lost handset. The regulation/ direction of blocking of IMEI should be supported by legislation to prevent re-programming of IMEI number. The following laws laid down in the Information Technology Act, 2000 should address the unlawful reprogramming and tampering of original IMEI numbers on GSM handsets:

2. Definitions

(1) In this Act, unless the context otherwise requires, —

(i) "computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

OFFENCES

65. Tampering with computer source documents.

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.—For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Mobile devices are becoming advanced microcomputer with advanced computing capabilities. These devices are can be classified as computers given in the above definition in the Information technology Act, 2000. The reprogramming or tampering of IMEI would be classified as an offence under Section 65 read with Section 2(i) of the Information technology Act, 2000.

This above law can be only be effective when it is enforced and unscrupulous elements engaged in the reprogramming/tampering of IMEI are booked under these laws. For this purpose close coordination between law enforcement agencies and TRAI would be pre-requisite.

8) What should be the procedure for blocking the IMEI?

The procedure should not be that stringent so as to in convenience the customer. The process can be bench marked against the methodology adopted by the credit card companies to block the credit card.

When mobile equipment is stolen or lost, owners can typically contact their local operator with a request that it should be blocked. The local operator possesses an Equipment Identity Register (EIR), which then puts the device IMEI into it, and can communicate this to the Central Equipment Identity Register (CEIR) which blacklists the device in all other operator switches that use the CEIR.

The blocking of IMEI may be done by CEIR maintenance agency based on Mobile owners identity proof

9) If lost mobile is found, should there be a facility of unblocking the IMEI number? If yes, what should be the process for it? Should there be a time limit for unblocking the IMEI number? Should it be chargeable?

The customer may elect unblocking the handset in the event the phone is found or recovered. If the reported lost or stolen handset has been recovered the customer will need to contact the service provider and request the handset to be unblocked. The unblocking will be allowed subject to same customer verification procedures used when the handset was originally blocked. A time limit of 48 hours may be allowed after completing verification process for unblocking IMEI.

Service providers should be allowed nominal charges for unblocking of IMEI.

* * *