Association of Unified Telecom Service Providers of India

AUSPI/12/2010/249 15th December, 2010

Dr J S Sarma,
Chairman,
Telecom Regulatory Authority of India,
Mahanagar Door Sanchar Bhawan,
Jawaharlal Nehru Marg,
New Delhi.

Sub: AUSPI's Response to TRAI Consultation Paper No.14/2010 on Issues relating to blocking of IMEI for lost / stolen mobile handsets

Dear Sir,

We are pleased to enclose herewith AUSPI's Response to TRAI Consultation Paper No.14/2010 on Issues relating to blocking of IMEI for lost / stolen mobile handsets.

AUSPI requests the Authority to kindly take our views into consideration while framing its recommendations on the subject.

Thanking you,

Yours faithfully,

S.C.KHANNA
SECRETARY GENERAL

Encl: As above

Copy to:

1) Shri R. Ashok, Member, TRAI
2) Prof. H S Jamadagni, Member, TRAI
3) Shri R. K. Arnold, Secretary, TRAI
4) Shri Sudhir Gupta, Pr. Advisor (MN)

B-601, Gauri Sadan, 5, Hailey Road, New Delhi - 110 001
Tel. : 23358585, 23358989 Fax : 23327397
E-mail : auspi@auspi.in Web : www.auspi.in

AUSPI'S RESPONSE TO THE TRAI CONSULTATION PAPER NO.14/2010 ON 'ISSUES RELATING TO BLOCKING OF IMEI FOR LOST /STOLEN MOBILE HANDSETS'

PREFACE

The mobile phone industry is developing at an incredible pace and today's feature rich handsets provide users with access to products and services which we would never have dreamed possible a decade or so ago. Increased pressure of competition in mobile telephony sector has led to competitive tariffs, which in turn have spurred telecom growth and increased teledensity. With the growing importance of mobile phones and variety of new applications, the handset has become a valuable item particularly in terms of the personal data/information stored in it. Moreover, the mobile phone handsets, with new technologies such as 3G and with advanced features and applications, are still coveted in the market.

With all technology solutions, some risks emerge to the end users of product and service offerings, particularly those that provide us with the ability to connect with the global community. It must be stressed that these risks are not new, they are simply applicable to a new operating environment. While most of us have a strong desire to enrich our lives by participating in this bigger environment, it is important that we are aware of the risks of mobile phone ownership. These risks range from that associated with personal safety and the release of personal information about ourselves when communicating with others.

The mobile phone theft is a serious problem world over. In India also, with increased penetration of mobile services, it is becoming a problem especially in the Metros and urban areas which have become some of the hunting grounds for mobile phone lifters. The emphasis in developing these new products and services is always designed to enrich the customer experience, however there are always isolated experiences which remind us that any new technology product can carry with it a certain amount of risk if not used responsibly.

GENERAL

AUSPI supports the TRAI initiative relating to the blocking of IMEI for lost / stolen mobile handsets.

The International Mobile Equipment Identity (IMEI) is a unique serial number **which identifies the GSM handset only** and not CDMA handsets.

RE: CDMA DEVICE

ESN is a unique serial number which is given to CDMA devices unlike GSM where all devices are SIM based. For CDMA, there are two types of 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 centre can check the call's validity and 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. Since UIMID is placed on RUIM and not on the handset, tracking /blocking a stolen/lost CDMA handset will not be possible.

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

RE: GSM DEVICE

i. The IMEI is used only for identifying the device and has no permanent or semi-permanent relation to the subscriber (unlike the ESM of CDMA). 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.

ii. In rapidly growing mobile market, there are millions 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.

iii. It may be desirable to first assess the extent of the problem that is caused by reprogrammed IMEI numbers before putting in place a mechanism to address the same. For example, 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 difficult to prove that reprogramming is carried out.

We request that the following important issues need to be looked into, analyzed and transparently discussed before finalization of the regulation:

- **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.**

REPONSE TO THE ISSUES RAISED IN THE CONSULTATION PAPER

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

- 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 have been 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 onetime 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 centre 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*

IMEI implementation will not increase load. However mobile phone should not be allowed to be retained indefinitely in the list. Considering the short life span of mobile phones the maximum period for retention of any IMEI should not be more than 6 months to one year.

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

The Central Equipment Identity Register which is an IMEI DB(database) system is the central system for network operators (those that have an EIR) to share their individual black lists with one another so that service is denied for the particular device that appear on that blacklist.

The CEIR should be maintained by NIC/DIT as is the case with Do Not Call Registry (DCR). Other efforts are also going on in other countries, such as the establishment of a global Central Equipment Identifying Register (CEIR) at Dublin, Ireland, and a "Mobile Industry Crime Action Forum" representing Operators, Manufacturers and retailers for tackling mobile phone theft and related issues.

A major effort is required to build up such a database, and co-operation of all concerned including internally would be crucial for its effectiveness. However, the establishment and maintenance of the database is crucial to the exercise as this would mean that once a customer has reported their phone as stolen or lost to their network operator, the phone would be blocked from use across the Globe. This would significantly reduce the incentive for stealing mobile phones and stop the problem simply being displaced from one country to another. Also, to the extent that the database is available, police authorities could also use it for their purposes.

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. es.

Taking the mobile subscriber base in the country to be around 700 million at present, a theft/lost rate of 1%, i.e. about 10 million capacity may 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?*

For implementing the given scheme, a number of steps namely preparation of database of all the available IMEI's, regular updation of database in the EIR, creation of CEIR and its regular updation will be involved. This will involve participation by all the service providers operating in the country. Moreover, a Central Equipment identified Register (CEIR) will need to be created and regularly updated. All this will involve certain cost and constant monitoring.

NIC/DIT may indicate the CAPEX and OPEX estimate for the same.

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?*

Many countries have acknowledged the use of the IMEI in reducing the effect of mobile phone theft. There are several Acts being practiced in other countries which widen the categories of persons who can be proceeded against, under the Mobile

Telephones Re-programming. These Acts are created to counter the number of criminal offences relating to the electronic identifiers of mobile wireless communications devices. For example, In the UK, a law (Mobile Phones Reprogramming Act 2002) has been made to curb the reprogramming of handsets. Reprogramming would make possible re-use while making it difficult to identify any theft of the handset or possessing equipment that can change IMEI. In Latvia, such an action is also considered a criminal offence. Mobile operators are also encouraged to take measures such as the immediate suspension of service and the replacement of SIM cards in case of loss or theft.

Apart from UK and Latvia which has already addressed this issue by making re-programming of mobile handset as an offence, some other countries like France, Germany, Greece, Spain etc., are actively considering solutions in partnership with the Police authorities on this issue. For India too, therefore, we need to take a close look at the need for taking such steps. An important issue in this regard, is whether reprogramming should be cognizable offence, and whether the existing police structure would have adequate incentives to vigorously pursue such thefts.

We consider that the provisions in the Information Technology Act, 2000 are sufficient to prevent reprogramming of mobile devices. The relevant provisions are as follows:

Quote
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;

Unquote

Quote

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.

Unquote

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

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

The blocking of IMEI may be done by CEIR maintenance agency based on following documents.

1. Mobile owners identity proof
2. FIR copy as proof that mobile is stolen / lost

An authorization needs to be carried out if the complaint is made by other than owner.

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 be unblocked. As the customer is required to confirm certain information relating to the handset usage, call records as a means of verifying the customer and the handset IMEI can be used. The unblocking may be taken place within 72 hours subject to customer verification procedures used when the handset was originally blocked. The same person who requested the block must also request for the unblocking.

No, the unblocking of IMEI should not be chargeable; however penalty for every attempt with the wrong IMEI may be imposed.

****