Consultation Paper No. 14 /2010

Telecom Regulatory Authority of India

Consultation Paper

on

Issues relating to blocking of IMEI for lost /stolen mobile handsets

New Delhi: 2nd November, 2010

Preface

With increasing penetration of mobile services, and the growing importance of mobile handsets, loss of a mobile phone is emerging as a serious concern to the consumers, because of valuable personal data stored in it. Presently, there is no mechanism in place to block a lost mobile phone. Although, TRAI had initiated, in the year 2004, consultation on the issue, the matter was not proceeded further as several service providers did not have the capability in their network to track/block the handsets.

The purpose of this consultation paper is to revisit this issue in the interest of consumers. All stakeholders are requested to send their comments, preferably in electronic form, on the issues raised in the consultation paper by **30th November, 2010**. Comments will be posted on TRAI's website as and when they are received. Counter comments, if any, to the comments may be sent to TRAI by **7nd December, 2010**. For any clarification/ information, Shri Sudhir Gupta, Pr. Advisor (MN), TRAI, may be contacted at Telephone No. +91-11-23220018 Fax No. +91-11-23212014 or email at pradvmn@trai.gov.in or trai.mn@gmail.com.

(Dr. J. S. Sarma)
Chairman, TRAI

Issues relating to blocking of IMEI for lost /stolen mobile handsets

Background

1. As on 31st August 2010, there were 670.61 million wireless connections in the country and around 18 to 19 million connections are being added every month. 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 expensive in the market.

2. 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 where areas such as Market place, Malls, Cinema Halls, buses, railway, metro stations /trains have become some of the hunting grounds for mobile phone lifters.

3. Today, in case of theft of a mobile phone, on complaint the service providers are providing the facility of blocking the SIM card. In order to block SIM card, the subscriber need to report the theft to the service provider's call centre. The call centre personnel verify the identity of the subscriber and the lost SIM is blocked in their system, thereby disabling all services for the reported lost SIM. A duplicate SIM is provided to the customer as per the provision. Though the service providers through these actions ensures that the mobile connection is not misused, however, it does not take any action either for blocking the handsets or for tracking its usage. Although, for the lost handset, customer can file a report to the police but recovery rate of lost handset is dismal, since the size of these handsets are small and can be easily hidden.

The Technical Terms used in this context

International Mobile Equipment Identity (IMEI)

4. International Mobile Equipment Identity (IMEI) is a unique serial number which identifies the handset. The IMEI can be found inside the handset below the battery or by entering *#06# in most GSM handsets. Unlike in GSM where all devices are SIM based, there are two types of devices that CDMA sell in Indian market namely Non Removable User Identity Module (Non-RUIM) and Removable User Identity Module (RUIM). These handsets have unique identification namely Electronic Serial Number (ESN). ESN can be found inside the handset below the battery.

Equipment Identity Register (EIR)

5. IMEI /ESN numbers are stored in the EIR database of a service provider. In case of a complaint regarding theft of a handset, the service provider can flag the IMEI number of the handset and can block the handset in its own network. If the EIRs of service providers are shared through a centralized database, the lost / stolen mobile can be prevented from use in all networks. Generally, such database is known as Central Equipment Identity Register (CEIR)

TRAI initiative

6. In order to curtail the illegal handset market, discourage handset theft and protect consumer interest, TRAI had earlier initiated a preliminary consultation paper on 8th January, 2004. However, at that time, many service providers were not having the capability to track/block IMEI through Equipment Identity Register (EIR). EIR is a database deployed in a network of service provider, which store the IMEI/ESN of the handsets used by subscribers. Moreover, COAI also informed the Authority that there are many issues both technical and administrative which do not make it feasible

to block the IMEI. Further, IMEI numbers of handsets could be changed through reprogramming and hence there could be many handsets in the market, which has been sold/reprogrammed after theft. Therefore, at that time, mandating the facility of blocking of the IMEI number for lost/stolen mobile was not considered as an immediate solution. Now, the purpose of this consultation paper is to revisit the issues related to blocking of mobile handsets using its IMEI number

DoT's Direction on IMEI /ESN

7. In the year 2008, it was observed that a large number of mobile handsets are either working without any IMEI / ESN or having all zeros. Such mobile handsets are security risk as they cannot be traced by the security agencies. Further, it was noticed that the networks of many service providers are not fully equipped with EIR for tracking the IMEI of the handset. Therefore, in the interest of security, all Access Service Providers were directed by DoT on 6th October 2008 to make provision of EIR in their systems so that calls from mobile handsets without IMEI or that of IMEI with all zeros are rejected. Subsequent to this direction, all service providers have upgraded their network and presently they have provision of EIR in their network.

8. As mentioned above, the service providers can block the handset in its network if it has the capability of EIR. However, to block its usage in all networks, a centralized equipment Identity register will need to be created.

Blocking of IMEI

9. The, EIR contains the list of IMEIs of all the subscribers. This list can be classified into white list (Genuine), Blacklist (Unauthorized). When the EIR receive a request from the Mobile Switching Center / Visitor Location Register (MSC/VLR), it will search its database to determine on which list the Mobile's IMEI is located. It will then send the information back to the

MSC/VLR, which acts on the information accordingly e.g., the MSC/VLR may terminate the call if the Mobile IMEI is found in the black list. CEIR is a system that can integrate the IMEI information of EIRs of all the networks.

10. The EIRs of operators will be updated periodically by CEIR so that the blocking can be done in all networks. Thus, black listing the IMEIs of all the stolen mobile phones and blocking their use in all VLRs is an effective way of reducing mobile phone thefts. However, from the commercial perspective, this involves cost both in terms of CAPEX & OPEX as centralized database need to be established and maintained. Further, there is a possibility of network delays as a query will take place with EIR on call by call basis, especially, in the post MNP scenario wherein every call is to be dipped into MNP database.

11. For creation of CEIR, the following options can be considered:

(a) CEIR be jointly maintained by service providers or through their associations

(b) CEIR be maintained by a third party

12. The issue for consideration would be the source of funding for establishing and maintaining the CEIR

Issues in implementation:

13. As explained in the preceding paragraphs, a centralized database is required which will be the repository of all blocked IMEIs. In this regard, issue also arises whether such database should be established centrally or zonally. In the case of central database, only one national level CEIR will be maintained. As this contains repository of blocked IMEIs of all circles the size of the database could be very large. In case of zonal database, there will

be the issue of interconnecting them so as to make the data regarding blocking of IMEIs of all the zones available to telecom service providers.

14. The next issue is about recovery of this cost incurred in the options mentioned above. In both the options, the issue would be whether the operator should absorb the cost incurred or the operators should recover the cost from customers for providing facility of blocking the IMEI.

15. Presently, most of the mobile devices are software based and therefore easily re-programmable. Therefore, in spite of IMEI blocking, the IMEI of the handset could be changed through re-programming. United Kingdom (UK) for example have a legislation to prevent the re-programming of mobile phones under the Mobile Telephones (Re-programming) Act, 2002. In India, although theft of mobile phone is a criminal offence covered under the existing laws, there is no specific legislation to prevent re-programming. This issue was deliberated with the service providers during the consultation process on this subject in the year 2004 and subsequently in a meeting with the telecom service providers this issue was raised in the year 2008 wherein service providers had emphasised that a suitable legislation is required to address the issue of re-programming of the handsets.

Facility of Unblocking the IMEI Number

16. In case the reported lost or stolen handset has been recovered by the subscriber, a facility can be extended to him to unblock the IMEI number within certain period from the date on which his IMEI is blocked, so that the handset can be reused. The issue in the context will be whether any time frame should be specified. Regarding the procedure for unblocking, the Subscriber may approach his service provider and request for unblocking. The same person who had requested the blocking of IMEI may request for its

unblock. In this context, another issue will be whether the facility of unblocking be also made chargeable.

Mobile Tracker facility:

17. Now a days a handset feature called mobile tracker is available in some of the mobile handsets. In these handsets, an application resides in the handset. Every time a new SIM card is inserted in the mobile phone, two pre-selected SIM numbers automatically receive a prompt informing the contact number of the new user. This facility enables the customer to inform the police while reporting the mobile theft, the contact number of the individual who is using the lost/stolen mobile handset. However, only a few handsets have tracking feature. Therefore, awareness can be generated among mobile subscribers to encourage use of such applications in their mobile handsets to curb mobile theft.

International Practices

18. In some of the countries, the mobile theft is discouraged by maintaining the Central Equipment Identity register jointly by operators. In UK the legislation is in place for re-programming of mobile phones. Some of these examples are discussed in the following paragraphs:

a. Australia

In Australia, when a handset is lost or stolen, customer can report to their service provider not only to bar the SIM card but also to block the handset from further use across all networks. The new user is therefore unable to make or receive either text or voice call, even if a new SIM card is inserted (with an exception of emergency calls). Service provider performs the customer verification procedure to ensure that the correct handset is blocked and to prevent fraudulent blocking of other people's handsets. Customer can verify whether the IMEI number has been blocked through website managed by Australian Mobile Telecommunications Association.

b. France

France regulator ARCEP mentioned in their annual report for the year 2003 that Anti-theft measures were reinforced for improved effectiveness. Operators in metropolitan France were obliged to put the IMEI numbers in a centralized database for identifying terminals that have been declared stolen and to block the terminals accordingly.

c. Pakistan

The Pakistan Telecommunication Authority (PTA) placed a technical system to curb mobile phones snatching with the help of cellular mobile operators, city police liaison committee, federal and provincial police departments and other government functionaries. The mobile operators have installed equipment identity register (EIR) system which enables a stolen or snatched cell phone to be blocked through its IMEI. EIR will block the handsets once the snatching or theft is reported by the customer. PTA has also developed a standard operating procedure to be followed by all concerned including the mobile phone operators to streamline the reporting of stolen or snatched cell phones. PTA has also launched awareness campaign to educate the telecom users about the reporting of snatched or stolen mobile phones. Before registering a complaint a consumer is required to make sure the mobile connection is in his/her own name and will provide IMEI number along with own number, ID/ Address etc. The system will block the handset and it cannot be re-used. Mobile companies update their database of stolen mobile sets, which will be shared by all provinces.

d. Philippines

In Philippines, a Senate Bill titled "An act to create offenses in respect of unique electronic equipment identifiers of mobile wireless communications devices" was filed on July 12, 2010. The Bill is yet to be approved by the Legislative Committee. The Bill comprises the following points:

1. Reprogramming mobile telephone: A person commits an offense if:

   a. He changes a unique device identifier, or
   b. He interferes with the operation of a unique device identifier.

A unique device identifier is an electronic equipment identifier which is unique to a mobile wireless communications device.

2. Possession of anything for re-programming purposes: A person commits an offense if:

   a. He has in his custody or under his control anything which may be used for the purpose of changing or interfering with the operation of a unique device identifier, and
   b. He intends to use the thing unlawfully for that purpose or to allow it to be used unlawfully for that purpose.

3. Supply of anything for reprogramming purposes: A person commits an offense if:

   a. He supplies anything which may be used for the purpose of changing or interfering with the operation of a unique device identifier, and
   b. He knows or believes that the person to whom the thing is supplied intends to use it unlawfully for that purpose or to allow it to be used unlawfully for that purpose.

4. A person found guilty of an offense under this Act is liable to imprisonment for a term not exceeding five years and/or to a fine not exceeding P 20,000

5. But a person does not commit an offense under this Act if:

a. He is the manufacturer of the device, or
b. He does the act with the written consent of the manufacturer of the device.

e. Poland

In Poland, according to the Telecommunications Law, the mobile operators need to comply with the obligation to block IMEI numbers of stolen handsets. The law imposes the following obligations on mobile operators:

1. To prevent the use of stolen mobile handsets in their network.
2. To transfer information identifying stolen handsets to other mobile operators in order to enable their blocking.

In order to fulfill the obligations, the mobile operators have signed an agreement specifying conditions for cooperation between mobile operators with respect to the exchange of information enabling the identification of stolen telecommunications terminal equipment. The agreement has introduced uniform principles of handling requests for blocking/unblocking an IMEI number, form of "Request for blocking/unblocking terminal equipment" as well as a specimen "Certificate of reporting/withdrawal of a report to the police on the theft of terminal equipment".

According to the law, on submitting a request for blocking a mobile handset, the following documents are required:

1. A certificate of reporting the theft to the police.
2. A document confirming one's property right with regard to a blocked mobile handset (together with an IMEI number), such as: a VAT invoice, a receipt, a guarantee card, an agreement for the provision of telecommunication services or an annex to this agreement, a sales contract or a contract of donation together with an original proof of ownership (an invoice, a receipt).
3. A document confirming the applicant's identity.

4. An authorisation in the case when a request is submitted by a person authorized by the subscriber.

Although the provisions of Telecommunications law mention only the blocking of stolen handsets, operators under the agreement offer a complementary service of unblocking previously blocked handsets, applying the same procedure as in the case of blocking IMEI numbers.

f. Turkey

In Turkey, the Information and Communication Technologies Authority established a call centre namely the Information and Denouncement Centre (IDC) under the provisions of its law. People who lost their devices via stealing, loosing or in any other way, denounce the IDC by calling it directly or applying to the offices of public prosecutor.

Central Equipment Identity Register was established in order to register the legally imported devices and disconnect the smuggled, lost and stolen devices or the ones with cloned IMEI number from electronic communication network. In this scope, various applications were developed thereby many transactions will become automatic and the process will run effectively, accurately and rapidly which directly affects mobile phone users, GSM operators, importers etc.

In this scheme, the Call Centre receives the applications of lost/ stolen device. The received requests are sent to the concerned GSM operator on condition that the identification information is confirmed. Following the confirmation by the concerned GSM operator, blocking of handset takes place through the CEIR.

g. UK

UK retailers and network providers have put in place a database to block stolen phones. The five major mobile phone networks in the UK (includes Vodafone, O2, Orange, T-Mobile) have a mechanism to block stolen phones across all networks within 48 hours of the home network being notified, thus rendering the handset useless in the UK. Further, legislation was in place under which re-programming of mobile handset is an offence. The Mobile Telephones (Re-Programming) Act 2002 made provisions to prevent the re-programming of mobile telephones, which involves changing the 'unique device identifier which is the IMEI number. When a lost /stolen mobile phone is blocked, unscrupulous individuals change the IMEI number and make it work again. This practice is illegal and only the manufacturers are allowed to alter it. Buyers can search online databases to see whether a phone has been reported as lost or stolen. Under this act, convicted person is punishable upto 5 years imprisonment or a fine or both.

As per the available information, apart from the above countries, the telecom service providers in Austria, Cyprus, Denmark, Finland, Italy, Sweden, Estonia and Ireland maintain CEIR wherein all operators are its members.

Summary of issues for consultation

1. In order to reduce/discourage mobile theft do you think the blocking of IMEI is an effective solution? Please give reasons
2. In case blocking of IMEI is implemented, to what extent load on the network will increase? Please give details
3. In your opinion who should maintain the CEIR? Please give reasons
4. Should the CEIR be maintained at national level or zonal level? Provide details including the estimated data size
5. Please comment on cost and funding aspects of Centralized EIR ? Please provide detailed cost estimates?
6. Should blocking of IMEI /ESN be chargeable from customer? If yes, what should be the charge?
7. Please give your views on bringing a legislation to prevent re-programming of mobile devices? In your opinion what are the aspects that need to be covered under such legislation?
8. What should be the procedure for blocking the IMEI?
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?