Consultation Paper No. 2/2004 dated 8th January 2004

TELECOM REGULATORY AUTHORITY OF INDIA

Preliminary Consultation Paper

On

Mobile Phone Theft

NEW DELHI

January , 2004

Preface

Mobile phone theft and its re-use is becoming a major problem in all countries. This also has a serious security dimension. In India too, despite rapid growth of the mobile telephony market, there is still a wide gap in the costs of handsets in the grey market and the legitimate market. The problem of theft of handsets in cities, specially metros is becoming a concern. TRAI has been considering for sometime the need to evolve a regime to disincentivise theft of handsets through legislation and other policies.

This paper provides a background framework for public consultation process with the stakeholders on the above issue in order to obtain feedback and suggestions to be considered by TRAI when it formulates its recommendations.

The Authority invites written responses from all stakeholders latest by 31st January 2004. It would be appreciated if the response is accompanied with an electronic version of the text through E-mail.

For further clarifications please contact Shri Sudhir Gupta, Advisor (QOS) Tel. No. 26160404, Email Address : sgupta03@bol.net.in. The Fax No. of TRAI is 26103294.

(Pradip Baijal)

Chairman TRAI

Introduction

Increased pressure of competition in mobile telephony sector has led to competitive tariffs, which in turn have spurred telecom growth and increased teledensity. The cost of the handset is probably the main inhibiting factor at the low end of the market. Though this cost has also been falling steadily, there still is a gap between the prices in the grey market (consisting of stolen/smuggled handsets) and the legitimate market. In order to curtail the illegal grey market and protect consumer interest, some action is required to be taken to discourage this crime of handset theft.

This consultation paper addresses some policy initiatives, which may be taken to address the theft of mobile phones. Chapter 1 summarises some relevant aspects of the problem and list out certain findings and the current position of different countries on this problem. Chapter 2 takes up a solution adopted or under consideration in the United Kingdom and in other European countries. The applicability of this solution to India needs to be examined and inputs are requested from the stakeholders on this matter.

Chapter 1

Theft of Handsets and Certain Ongoing Efforts At the International Level to Deal With the Problem

Mobile phone instrument theft is becoming a major problem in all countries and is a key driver behind city crimes and robbery. Globally this is seen as a major issue and the problem is being studied to find an effective solution. 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. Other efforts are also going on, 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. In the European Union, data is being gathered by the UK through questionnaire responses to address the matter of mobile phone theft (please see Annex A). These various initiatives, including responses to the questionnaire in EU, show that a number of collaborative efforts are needed to tackle the problem of mobile phone theft.

Efforts need to be taken by various parties concerned, based on specific database, institutional structures, and co-operation among manufactures, Network Operators, and among Government agencies. In fact, there is a need for even collaboration among Governments to address this matter. Based on an examination of the efforts being made internationally, it is possible to identify some of the main factors/agents that have emerged as being important for tackling mobile phone theft. In summary, these include:

- **Data and Statistics** – Several countries do not hold mobile phone theft data. Database of the relevant phones which need to be tracked is an essential ingredient of any effective effort to curb the theft of mobile phones. A major effort is required to build up such a database, and co-operation of all concerned would be crucial for its effectiveness. In India, no authentic data is available regarding the number of mobile handsets stolen in a year. In those countries that have statistics on mobile phone theft, data is collected by the police, and the scale of the problem in some cases involves up to 330,000 stolen mobile phones a year.

- **Import/Export of Stolen Mobile Phones –** There is an international market for stolen mobile phones and an acknowledgement that these phones are being exported. However, there is no hard evidence or intelligence on the import/export of stolen mobile phones. There have been no joint operations between police forces from different countries to date.

- **Reprogramming activity –** Reprogramming makes it difficult to identify the original phone, because through re-programming the identification number of the phone, i.e., the International Mobile Station Equipment Identity (IMEI), is altered. Reprogramming is undertaken by independent mobile phone retailers/repair shops and private individuals. However, again, there is no hard intelligence on the scale and nature of reprogramming activity.

- **Legislation –** Reprogramming activity is illegal in a few countries and legislation is planned or under consideration in some others.

- **Co-ordination across Government –** There has been limited joint working across Ministries to tackle mobile phone theft to date.

- **Mobile Phone Industry** – In most countries, discussions with the mobile phone industry on addressing the problem of mobile phones have either not taken place or have only just begun and are at an early stage. Further actions to address mobile phone theft have therefore not yet been agreed.

- **Network Operators** – In some countries all network operators have joined the global database of stolen and lost phones whilst in others no network operators are participating in the Central Equipment Identifying Register (CEIR).

- **Manufacturers –** Discussions have either not taken place or are only just beginning. No forward actions have been agreed yet, either in terms of making the International Mobile Station Equipment Identity (IMEI) tamper-proof/tamper-resistant or in enhancing mobile phone handset security in other ways.

The issue of mobile phone theft needs to be addressed through a concerted effort made globally. The more countries take action, the greater the combined impact of this action. Countries need to work together collaboratively to tackle this shared problem as lasting change can only be secured through effective multi-country co-operation, such as the process initiated among European countries. During the period when efforts are being made for such collaboration, we should begin certain efforts within our own jurisdiction and look for various possible solutions.

Chapter 2

Suggestions For Solutions

The problem of phone theft is being addressed and/or tackled in different countries to varying degrees. Chapter 1 has shown that addressing the problem requires active participation and co-operation of the Government, law enforcement agencies and the mobile operators. Apart from UK 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.

If it is decided to address the issue of mobile phone theft in India, we should identify the main entities involved, the steps to be taken by them and the procedures for implementation of the relevant policies (both the particular policies and their sequence) within the country as well as in collaboration with Government and private sector in other countries. For such efforts, we need to take account of the insights that are achieved from the ongoing efforts in other countries, study the implications of the policies for our domestic entities, and tailor our own policies and procedures to our conditions.

In addition to the criminal act of theft of handsets, the issues that require to be addressed are:-

i) Blocking of SIM
ii) Prevention of re-programming of IMEI
iii) Ensuring the prevention of Import/Export of stolen handset. For this the following action requires consideration.

The various steps required for effectively addressing the problem include:

- **Identifying the main players involved** – It is necessary to identify the main players, e.g., operators, manufacturers of the handsets, police authorities, and other relevant Government authorities.

- **Creation of Global database** – There is a need to create a large database with the relevant information. This would include, for example, a Central Equipment Identity Register (CEIR), which would be a cross-country effort. An important issue to examine is who will maintain the CEIR. However, the establishment and maintenance of the database is crucial to the exercise, and countries whose networks operators have not already joined the CEIR should lobby their networks to do so as soon as possible. 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.

- **Procedures for implementation** – We need to devise the relevant procedures for data collection, exchange, and monitoring of data, role of the operators in reporting the stolen handsets, together with the various steps required for the relevant entities to interact with each other and collaborate in the process.

- **Reprogramming legislation** – The blocking system works by reference to the International Mobile Station equipment (IMEI) number of a phone. One way of circumventing the system therefore is to change (reprogram) the IMEI number of a phone. To support the CEIR, countries who have not already done so should consider implementing legislation to criminalise reprogramming activity. An important issue in this regard is whether re-programming should be cognizable offence, and whether the existing police structure would have adequate incentives to vigorously pursue such thefts.

- **Publicity for Public awareness** – These measures need to be brought to the attention of the general public and a publicity/media strategy needs to be implemented so that the public know what action to take if their phone is stolen and are aware that reprogramming mobile phones is illegal.

- **Joint police operations** – Police forces across the globe need to work together on joint operations to build intelligence on the import/export of stolen mobile phones, reprogramming activity and links to organised crime.

- **Improvement in handsets security** – The problem also needs to be tackled at source. Collective pressure needs to be applied to global manufacturers to ensure that they invest in developing a) tamper-resistant IMEIs

and b) a forward strategy for enhancing future handset security. This pressure should come from the government and also from the network operators and retailers in each country. A joint action by operators and retailers across the world against the purchase of non-secure handsets would make security a priority for manufacturers.

The above list encompasses a wide range of actions, and would be achieved only in the long run. If the problem of stolen handsets is to be addressed in the near future, we need to identify among these steps, those actions through which we could initiate the process, and still achieve substantial effectiveness. Two major such steps involve the blocking of SIM cards/handsets, and the creation of the relevant database. These are discussed below.

TRAI has earlier considered the process of blocking of SIM cards in case of theft of mobile handset. But by blocking of the SIM card by any particular CMSP will not give any relief against the reuse of the stolen handset. To minimize mobile handset theft, the blocking of the handset itself is a must. The handset blocking could be done on the basis of unique IMEI number of the handset. Sharing of IMEI numbers of lost handsets among all CMSPs in the country and their blocking by all operators would effectively curtail this theft problem. This can be controlled to some extent by having an integrated solution that would require:

- **Equipment Identity Register (EIR)**: EIR is a database deployed in a network to store the IMEI of the handsets used by subscribers. These IMEI numbers are stored on three lists, white, gray and black, indicate the current status of the mobile equipment:
  - ✓ **White list**- Indicates approved mobile equipment.
  - ✓ **Gray list**:-Indicates mobile under observation, such as for suspected malfunction.
  - ✓ **Black list**-Indicates mobiles denied access to the network, such as stolen or missing mobiles.

IMEI checking is executed to find out if the mobile equipment on some of the lists or if it is completely unknown in the EIR.

- **Central Equipment Identity Register (CEIR**): CEIR is a central data base which integrates the EIRs of all the networks containing information on serial number (IMEI) of all the handsets that have been approved for use on GSM networks and are in use in the country.
- **How does it work :** When the EIR receives a request from the MSC/VLR (or SGSN), it searches its data base to determine on which list a Mobil IMEI is located. It then sends the information back to the MSC/VLR, which acts on the information accordingly e.g., the MSC/VLR may terminate the call if the Mobil IMEI is found in the black list.

  EIRs that are registered users of the CEIR dial-in directly or over a secure Internet connection every day to share latest lists of black listed hand sets with other operators. Every night, the CEIR takes all the black lists from different operators of a country and adds them together into one big Black list. When an EIR connects to the CEIR the following day, it down loads the Black list for its own use. By loading that big Black list onto the local EIR, all handsets reported as stolen on all other connected networks all over the country up to the previous day are now blocked on that network also.

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. Furthermore, the CEIR interface of all the EIRs can be used to expand the coverage in an inter-network level as well as internationally.

The effectiveness of any solution will depend upon a combination of a technical solution, active cooperation and the partnership of the local police/law enforcement agencies, and an effective campaign to educate the public/mobile handset users.

Chapter 3

Issues For Consideration

Based on the previous Chapters, we may consider the following issues for comments and further examination:-

1. **Role of Regulator:** The subject of theft of mobile handsets comes under the purview of Law and order which is a state subject in our country. Should TRAI take initiative in mobilizing public opinion, drafting legislation and encouraging the service providers and vendors to take action for minimizing this crime?
2. **Grey Market**: In the rapidly growing mobile sector, already more than a million subscribers are estimated to be having handsets from the Grey market. In case, action is taken by the service providers to block the handsets having duplicate IMEI, then a mechanism needs to be evolved and put in place to decide the fate of these subscribers on an individual basis. Suggestions on such a mechanism are requested.
3. **Procedures required for collection/updation of data and interaction amongst the relevant entities** : It is necessary to devise procedures for collection and use of data as well as the interaction of operators, consumers and other stakeholders in this exercise. These procedures should be easy to implement and not impose great costs on the persons/institutions involved.
4. **Ownership and cost implication of setting up of CEIR** : 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. It needs to be deliberated and decided whether this control should be done by an agency like OMBUDSMAN or by some association like COAI, or by the Regulator i.e., TRAI.

5. **Legislation :** **A**part from blocking all the handsets, a legislation making re-programming of IMEI as an offence is also required so that the recycling of handsets after changing the IMEI is deterred. Countries like France, Germany, Greece, Spain are already considering making it an offence. In India also a legislation on the same lines may be required to be enacted in order to make reprogramming of handset for the purpose of changing the IMEI as an offence. Please comment.

The comments should relate to the relevant issues pertaining to both GSM and CDMA technologies.