Bryan Whittle
Director

www.telcordia.com

Telcordia Technologies, Inc.
One Telcordia Drive
Piscataway, NJ 08554

M +1 732.535.8675
bwhittle@telcordia.com

December 15th, 2010

Principal Advisor (MN)
Telecom Regulatory Authority of India
Mahanagar Door Sanchar Bhawan
Jawahar Lal Nehru Marg (Old Minto Road), New Delhi-110002

Kind Attn: Mr. Sudhir Gupta

Subject: Consultation Paper on Issues relating to blocking of IMEI for lost/stolen mobile handsets

Dear Sir,

Telcordia Technologies, Inc. is pleased to provide the attached response to your Consultation Paper No. 14/2010 dated 2nd November, 2010.

In case you require any further clarifications, please do let us know.

Yours Sincerely,

Bryan Whittle
Director
Telcordia Technologies, Inc.

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

Telcordia Response

Telcordia believes that a centrally managed registry for IMEI registration and blocking is a critical and necessary solution if India seeks to implement a comprehensive scheme to combat and thwart theft of mobile devices and services.

However, there are several factors that must be taken into account in its deployment to ensure the viability of such a solution. First, its effectiveness will critically depend on all operators participating. Further, operators must participate in a uniform fashion, implementing the system consistently through their varied networks, otherwise gaps and differences can be exploited for illicit purposes. In addition, the data required to construct a viable solution must be submitted by the operators to the CEIR in a timely fashion, cover their entire subscribership, and account for differences in core network technologies (e.g., CDMA MEID and ESN identifiers must be included as well as GSM IMEI and IMSI data).

The effectiveness, and cost effectiveness, of a CEIR can be increased by employing it for a broad set of use cases for detection and blocking of IMEI. In addition to handsets without an IMEI or with an IMEI of all zeros, known stolen and lost handsets should be placed on a blacklist to be shared with operators via the CEIR. Thus any handset on the blacklist can be blocked by whichever operator the handset is being used with.

Expanding use cases further, an IMEI value not appearing on the blacklist as being lost or stolen might be in use by many clone handsets. Such handsets can be identified or detected, then added to the blacklist in accordance with industry agreed rules. Blocking clones can protect citizens from acquiring counterfeit goods, identify and block illicit fixed-mobile termination infrastructure, and protect operator networks from poor quality handsets.

India should also consider the mitigation of theft for export, as stolen handsets blocked by the CEIR may consequently be exported to other markets for use. For the most expansive solution, India should consider seeking inter-national cooperation and licensing arrangements with other regulatory organizations and industry organizations, such as the GSMA IMEIDB, to deter migration of stolen handsets across nation-state boundaries. This can both deter theft for export and mitigate national security concerns surrounding the migration of handsets into India.

Effective reporting of lost and stolen handsets is critical to the effectiveness of a CEIR in building an industry blacklist. Thus a widely available, well marketed, and flexible reporting infrastructure must be established for this purpose. Subscribers, law enforcement agencies, and authorized third parties such as insurance companies, manufacturers and wholesale handset distributors will need the capability to report lost, stolen, or illicit devices, either via an operator or to the CEIR directly, with appropriate access and auditing controls.

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

Telcordia Response

To the extent that operators are already querying their EIRs for all handsets active on their networks, there will be no extra load on the signaling network. Any additional load will be on operator EIRs and the EIR to CEIR network for the processing and exchange of IMEI list data. In normal operation, only incremental list data need be exchanged. A bulk synchronization mechanism can be included for infrequent use to restore systems or populate new systems. The size of the list data load in terms of transmission facility needs depends on the traffic pattern (*e.g.*, whether a real-time trickle is used or a batch file is transmitted during a daily time window).

To the extent that operators are not yet querying their EIRs, the load on the signaling network will increase. In standard MAP protocol procedures, VMSCs create and send Check_IMEI messages to the EIR and receive and process Check_IMEI_Acknowledgement messages from the EIR to convey handset blocking status to the VMSC. The load and required link capacity per 1 million subscribers for such an exchange can be estimated as follows:

- Assumption: IMEI is checked only at IMSI attach/location update times.
- Assumption: 1 IMSI attach/location update per hour per subscriber.
- This gives 1000000 / 3600 (sec) ~ 300 Check-IMEI messages per second.
- Assumption: Each Check-IMEI is about 60 octets in size on an SS7 link.
- This will give a total SS7 link load of 300x60 = 18000 octets per second.
- Assumption: TDM links with a transmission capacity of 8000 octets per second are used at up to 40% of capacity.
- Therefore the stated load requires 18000/(8000x40%) = 6 links.

Concerning per call delay, this can be obviated by checking at IMSI attach/location update times. This captures mobile power-on and SIM insertion events within the coverage area of a network as well as activated handsets entering a network coverage area from outside.

3. In your opinion who should maintain the CEIR? Please give reasons.

Telcordia Response

Telcordia believes that a neutral third party, accountable to the Government, should deploy and administer the CEIR infrastructure.

By employing a neutral third party to operate the scheme, fair and non-discriminatory access and operations between individual operators and the CEIR is ensured. This eliminates the possibility, or appearance, of anti-competitive behavior by any individual constituency in the system. Operators will be regarded as customers and will be served in a fair and equal manner according to a common Service Level Agreement. New entrant operators can join the CEIR community and be treated in an even-handed manner.

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

Telcordia Response

Both a national CEIR and zonal CEIRs are likely feasible. However, the most appropriate solution for India should take into account the details associated with certain key factors. These include the following:

- Effectiveness. How would data uniformity, integrity, and security be assured so there is comprehensive pan-India detection and blocking of stolen handsets? If zonal CEIRs are contemplated they must be interconnected in such a way as to discourage theft across zones. How would that be accomplished to meet the foregoing requirements?
- Industry cost structure. Is a single national solution or multiple zonal solutions more expensive to set up and maintain by their providers? How can the expense of interconnection for operators be minimized?
- Timely evolution. How should an industry process for streamlined evolution to ever more stringent requirements be designed? There must be a balance between allowing more parties to bring helpful contributions versus increasing the complexity of reaching and implementing business, technology, and operations agreements.

The data size for India IMEI blacklist records can be estimated as follows:

- Assumption: 700M subscribers.
- Assumption: 10% individual IMEI blacklist records.
- Assumption: Each record would be up to 0.5KB, depending on the data fields used.
- This will give a database size up to 70M x 0.5KB = 35GB database.

The database size can be expected to grow at least at the rate of growth of subscribers, say 25% per year. Increased use of multi-IMEI handsets will contribute further growth.

Both approaches are likely viable and, in consultation with the TRAI, Telcordia believes it can identify and deploy the most appropriate solution for the Indian market.

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

Telcordia Response

CEIR costs will be incurred for both set-up and for ongoing managed services. Set-up components include establishing the data center environments, system hardware and software, and providing implementation services including industry testing and training. Ongoing managed service components include operation of importing/combining/exporting updates from operator EIRs and other authorized sources, help desk, systems monitoring and management, billing, hardware/software maintenance, and onboarding new users.

Various CEIR cost recovery approaches can be contemplated. An important principle is that the expense should be borne equitably across the ecosystem. As part of that the burden on operators should not be unduly high. Contributing constituencies can include the following:

- Operators. The terms and conditions of CEIR contracts with operators can be standard for all operators in such a way that a fair and equitable process is maintained among all parties. The actual amount paid per operator would be according to industry agreed rules.
- Third parties. Establishing a role for the CEIR in the resale of mobile devices is critical for its success. Third parties such as authorized dealers, repair centers, insurance companies, and resellers of used handsets could be charged for access to the database to determine the blacklist status of a handset, as well as providing a service to their end customer in assuring the validity of the device in-country and validating its legitimate chain of custody.
- Manufacturers/Distributors. Manufacturers and third party wholesale handset distributors could be charged for bulk registration of stolen handsets, providing a disincentive to theft before introduction into the India market. Such registration can involve theft of large quantities of handsets for which charges could be set accordingly.
- Subscribers. Subscribers could be charged for blocking a lost/stolen handset and/or for unblocking of a recovered handset.

Telcordia will be able to provide a quantitative cost estimate for the CEIR when certain critical cost factors are resolved such as whether the system is national or zonal and the extent of access, analytics and reporting capabilities requested by the government for regulatory enforcement and national security/domestic intelligence purposes, which for both purposes we expect to be borne by the contributing constituencies listed above.

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

Telcordia Response

If subscribers find blocking of IMEI to be a useful service, they should be allowed to pay for it. There has to be a balance so as not to disincent reporting by a subscriber, thereby rendering the service less effective in discouraging theft.

Authorized third parties, such as wholesale handset distributors or manufacturers, could be charged for registration of stolen handsets. Such registration can involve theft of large quantities of handsets and charges could be set accordingly.

Charges as outlined above can contribute to cost recovery of the system and help distribute costs equitably across the ecosystem.

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?

Telcordia Response

Legislation making reprogramming of IMEI an offense can strengthen the effectiveness and legitimacy of the CEIR. Thus Telcordia believes that such legislation should be introduced as soon as possible. The recent action by the Philippine government in this area provides a viable starting place for India's legal framework.

However, Telcordia believes that it is not necessary to wait for legislation to be passed before starting to deploy a CEIR service under existing rules governing the use of valid IMEIs in mobile networks. In the event that legislation takes longer than the initial deployment of the CEIR service, the subsequent legislation and corresponding law enforcement agency regulations could be overlaid as an upgrade to the existing programs reducing/discouraging mobile theft.

Legislation must take into account that legitimate reprogramming of handsets exists today and should continue to exist. This allows handsets to be upgraded or to be made ready for another owner. In most cases no reprogramming of IMEI is implied. Legitimate parties that are thereby usefully contributing to the mobile ecosystem must be protected. Thus, any framework must distinguish illicit reprogramming of IMEI from legitimate reprogramming by authorized manufacturers, their distributors, and repair depots.

Telcordia believes there is value in tracking, identifying and potentially greylisting IMEIs suspected of use within cloned, reprogrammed or counterfeit devices in advance of any additional legislation and believe a rapid implementation would provide a valuable data source to assist the government in quantifying the problem and assist in adequately addressing it in future regulation or legislation.

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

Telcordia Response

First, the CEIR blacklist must be constructed. Blacklists should be loaded from operator EIRs into the CEIR database. Industry rules must be specified for operator EIR updates, including frequency, data fields, and format. Effective reporting of lost and stolen handsets is critical to the effectiveness of a CEIR in building an industry blacklist. A reporting infrastructure must be established for this purpose. Subscribers, law enforcement agencies, and authorized third parties such as insurance companies, manufacturers, and wholesale handset distributors will need the capability to report either directly to an operator or to the CEIR as specified by agreed industry rules that are published with broad visibility. India government agencies might need to incorporate blacklisted IMEIs of banned devices.

The CEIR should combine the inputs to the industry blacklist according to industry agreed rules. A combined blacklist should then be downloaded to each operator. Industry rules should be specified for incremental and bulk synchronization downloads.

In addition the CEIR can load white lists, such as the GSMA published IMEI ranges allocated to GSM handset manufacturers. In this context, a legitimate handset must be on the industry white list as well as not on the industry blacklist. An industry white list can be downloaded to operators alongside the industry blacklist.

Second, the operator copy of the CEIR database must be accessed by the operator network for handset status. That can be done at IMSI attach/location update times. This approach captures mobile power-on and SIM insertion events within the coverage area of a network as well as activated handsets entering a network coverage area from outside. In standard MAP protocol procedures, the operator VMSC queries its EIR with a Check_IMEI message. The EIR responds with Check_IMEI_Acknowledgement message conveying the handset status to the VMSC.

Third, the VMSC must be configured to block in accordance with industry agreed rules. For example, if the IMEI is found on the blacklist then the Check_IMEI_Acknowledgement message returns “blacklist” to the VMSC and the VMSC blocks. In addition, if the IMEI is not found on the white list the Check_IMEI_Acknowledgement message returns “unknown” to the VMSC and, if appropriate in terms of industry agreed rules, the VMSC can block.

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?

Telcordia Response

There should be a facility of unblocking the IMEI number. This enables subscribers to retain their investment in their handset. Further, the reporting infrastructure will be more effective if subscribers are incented to report because there is a known safety valve available for recovering a handset.

To the extent that subscribers find unblocking of IMEI to be a valuable service they should be allowed to pay for it. Such charges will contribute to cost recovery of the system and help distribute costs equitably across the ecosystem. However, any such charges must not be so high as to disincent reporting by the subscriber. There must also be safeguards against inaccurate reporting of IMEI numbers, as this will incur costs to recertify and unblock.

Given India's vibrant mobile device resale market, there should also be a service for confirming whether a device is currently blocked by the CEIR database, thus providing a disincentive to sellers peddling stolen or lost devices. An appropriate pricing mechanism should be determined for this service.