ORGANIZACION DE LOS ESTADOS AMERICANOS
ORGANIZATION OF AMERICAN STATES

Comisión Interamericana de Telecomunicaciones
Inter-American Telecommunication Commission

XIX MEETING OF PERMANENT CONSULTATIVE COMMITTEE I: TELECOMMUNICATIONS/ INFORMATION AND COMMUNICATION TECHNOLOGIES
August 30 to September 2, 2011
Mar del Plata, Argentina

OEA/Ser.L/XVII.4.1
CCP.I-TIC/doc. 2405/11
26 August 2011
Original: English

GSMA RESOURCES AND POSITION TO SUPPORT REGIONAL FRONT TO COMBAT THE THEFT OF MOBILE TERMINAL EQUIPMENT

(Item on the Agenda: 3.1.5)

(Information Document submitted by GSMA Latin America)

BACKGROUND

With more than 5 billion users worldwide, GSM mobile phones are an integral part of daily life for a significant portion of the global population.

The ability to remain connected is highly valued. Unfortunately, there are people who play on the aspirations of those who don't yet own a mobile phone, or others who would like a cut-price upgrade, by feeding a black market in handsets obtained through mugging and street crime. Several stakeholders in a number of countries and regions around the world are concerned at the increasing incidence of aggravated theft targeted at mobile users. This concern is heightened where organised crime becomes involved in the bulk export of stolen handsets to emerging economies experiencing rapid mobile growth.

GSMA has engaged in dialogue with regulators, governments, network operators and mobile handset manufacturers in order to find solutions to combat handset theft. This paper describes the GSM Association's contribution to the global fight against mobile phone theft with its multi-faceted programme of initiatives that includes the promotion of stolen device blocking, the upgrade and expansion of its global database of stolen handset identities, and engagement with manufacturers to make the electronic identities of mobile phones more secure to ensure the effectiveness of handset blocking.

GSMA Mobile Handset Initiatives

Whilst the problem of handset theft is not of the industry's creation, GSMA recognizes handset theft as being a major public policy concern for network operators and national authorities. It was as a result of heightened concern amongst industry stakeholders that GSMA developed a number of mobile handset theft initiatives in order to find solutions to address this problem and these are summarized below.

Blocking Stolen Devices

GSMA strongly believes that if lost or stolen mobile handsets phones can be rendered useless, they become worthless on the black market. If the market disappears, thieves will stop targeting mobile handsets as desirable consumer goods to be stolen and reused or resold.

Within the technical specifications, operators have the ability to block specific handsets from accessing their networks. The functionality was originally created to allow operators to disable mobiles that were not type approved or could cause interference on mobile networks. The mechanism relies on each handset having a unique electronic identity. This is known within the standards as the International Mobile Equipment Identifier (IMEI).

To control network access, operators can create databases within their networks – technically known as the Equipment Identity Registers (EIRs) - in which the electronic identities of handsets can be stored. Phones to be disabled can then be registered on a "black list". During the registration and authentication process that occurs whenever a handset attempts to connect to a mobile network the IMEI is checked against the database and if the IMEI is contained in the blacklist, access will be denied (Please see basic scheme in Annex D).

EIRs are increasingly used to block network access to handsets that have been reported as lost or stolen. Operators can prevent the use of stolen devices by maintaining a black list on their networks. However, as most countries now have more than one mobile network, isolated databases on individual networks are ineffective in preventing the use of stolen handsets as blocking by a single operator will still allow those devices to reconnect to other networks by simply inserting a SIM card issued by a different operator. Operators can prevent the transfer of stolen phones from one network to another by sharing their individual black lists.

GSMA has facilitated the sharing of stolen IMEIs between operators since 1996 when it established the Central Equipment Identity Register (CEIR), now known as the IMEI Database and the benefits of using this solution are summarised below in Annex A. Participating operators regularly upload the latest changes to their own local EIRs to GSMA's IMEI Database. Operators can also download changes submitted by all other participating networks to create a local copy of the central database. By exchanging data daily, operators know that their local copy of the central database is never more than 24 hours old. Operators can configure their systems so that each time a mobile handset tries to access a participating network, its identity is checked against the operator's local database and handsets that have been black-listed by any participating network can be denied access.

Increased Need for IMEI Security

GSMA encourages its member network operators to deploy EIRs on their networks to ensure stolen handsets can be blocked by using the handsets' IMEI numbers. It is acknowledged that the effectiveness of EIR use is dependent on a secure implementation of the IMEI. Therefore, the use of EIRs does not represent the finite solution to handset theft and it is critical that EIR deployment should be complemented by the efforts of the handset manufacturing community to ensure that all handsets delivered to market incorporate appropriate security features. The enhancement of IMEI integrity should be designed to ensure the avoidance of fraud that will enable EIRs to work more effectively.

Although the GSM and UMTS technical specifications mandated that handset IMEIs should not be capable of being changed after the point of manufacture it became apparent that IMEIs were being

changed with relative ease for some years. The industry sought to avoid using standardisation as a means to deal with the IMEI integrity issue as standardised security solutions could stifle innovation and have the effect of equally exposing, rather than protecting, all products in the event of a compromise.

GSMA engaged with the device manufacturing community to resolve that situation and in 2004 concluded its work with the publication of detailed technical measures that must be implemented to increase the security of the IMEI against unauthorized change. The handset security technical principles (described in Annex B) provide guidance to handset manufacturers on how to secure the IMEI and provide operators with a set of criteria against which handset security can be assessed. This initiative, and the level of detail it entails, represents a significant improvement on the existing GSM specifications which did not contain any details or guidance as to how the IMEI should be protected.

It is acknowledged that security is not absolute and despite the best efforts of handset manufacturers it is possible that once secure IMEI implementations may be compromised at a later stage. Consequently, GSMA and the world's leading mobile handset manufacturers established a formal process to centralise the reporting and correction of newly identified IMEI security weaknesses to improve handset security levels during the manufacturing life cycle of current and future handset products. GSMA acts as a central clearing house for reports on handset models that are believed to have had their IMEI security compromised. These reports are referred to the relevant manufacturers, investigated, and responded to within 42 days. The reports contain details of proposed remedial action and dates from which equipment with new security measures will be introduced.

The commitment of the handset manufacturers to these initiatives has been very encouraging and most of the world's largest handset manufacturers formally signed up to support both initiatives. The support of a critical mass of handset manufacturers (named in Annex C) has been secured and efforts are on-going to have other manufacturers participate. GSMA is confident that the technical principles and the reporting and correction process will have a positive impact on IMEI integrity and will help increase confidence in the effectiveness of EIR use to block stolen devices.

Government Dialogue

It is important to note that IMEI security and blocking on its own is unlikely to be effective in fighting handset theft. IMEI blocking has had a positive impact in many countries but for a truly effective anti-theft campaign it is important that a holistic range of measures is put in place to ensure a multi-faceted approach is taken. National authorities have a significant role to play and it is critical that they engage constructively with industry on complementary activities and these include the following:

- Supporting regional and international databases to share stolen handset data rather than isolated local national databases that result in fragmentation;
- Promotion of handset blocking services to increase public awareness of the need to report stolen devices to service providers and to promote the message that stolen handsets will be rendered useless;
- Introduction of legislation to criminalise the unauthorised changing of handset IMEIs and the enforcement of that legislation to act as a deterrent for offenders;
- Compilation of handset theft statistics and related police intelligence data to ensure the scale of the problem and trends can be measured over time to ensure progress and effectiveness of countermeasures can be assessed;

- National authorities to exercise greater control over the importation of devices to ensure stolen devices from other jurisdictions are not being imported for use on local networks and that greater efforts are made to target the black market across the region.

GSMA has engaged with a number of governments and national and regional authorities around the world to assist with programmes and initiatives to combat handset theft. GSMA has recently worked extensively with the Colombian authorities and has shared the expertise it has gleaned from working with stakeholders in various jurisdictions to help shape its anti-theft measures. GSMA remains committed to work with the industry and government stakeholders in any CITEL member state and is willing to assist in any way it can to reduce handset theft levels.

Use of White Lists

In some cases national authorities have proposed and promoted the use of white lists to combat handset theft. GSMA considers whitelisting is not designed for that purpose as that is exclusively the function of the blacklist. GSMA has worked with industry and government stakeholders in over 100 countries on handset theft issues and very few countries have opted to use whitelists. Even in the counties where whitelists have been created there is no evidence that they have had any positive impact on theft levels simply because they are not intended to flag or deal with stolen devices.

The concept of whitelisting was developed to ensure that only legitimately produced devices with valid IMEIs can be used on networks. GSMA hosts a global whitelist of all IMEI number ranges that have been allocated to legitimate device manufacturers for implementation in their handset products. GSMA is the sole allocating body of IMEI number ranges so we hold the definitive list of genuine IMEIs that can be made available to network operators for use in their EIRs should they wish to deny access to illegal IMEIs.

In particular, GSMA considers whitelisting is not the best instrument for the following reasons:

- The compilation of local whitelists is not consistent or compliant with the global mobile standards;
- The creation of national whitelists impedes the free movement of mobile devices and undermines the fact that the vast majority of mobile handsets are produced for use around the world and not just in individual countries;
- In some regions of the world, the restrictive nature of local whitelists would be considered illegal as such lists could restrict the provision of goods and services across those regions;
- Tying specific customer IMSIs to IMEIs goes against everything that GSM stands for as it was the first cellular technology to separate the subscription from the device allowing users to change devices easily;
- Requiring registration of devices to individual user IMSIs, if this is proposed, prevents those users from easily changing devices or swapping SIMs from one device to another;
- Linking subscribers to IMEIs raises possible data privacy and protection issues that are not normally associated with IMEI data on its own that simply identifies equipment rather than individual users;
- EIRs do not have the ability to check and carry out an IMEI and IMSI comparison as only the IMEI is checked by EIRs so linking the two is of no benefit;

- If it is a requirement to carry out an additional association between the IMEI and IMSI this will have to be done as an additional check elsewhere within the network and this will impact call setup times to the detriment of the user experience and satisfaction with local mobile services;
- The IMEIs of stolen devices are likely to feature on whitelists if they were legitimately registered in the first instance thereby offering less benefit than a blacklist;
- Whitelisting at a local/national level can impact inbound roamers to the detriment of the local industry and the economy as a whole. Similarly, regular travellers between countries in the region that may swap SIMs when they enter a different jurisdiction with a local whitelist in place may experience service difficulties;
- Subsets of the global whitelist have no known positive impact on stolen handset use;

Whitelists can be effective in combatting the use of certain devices that should not be used on networks but national authorities and the industry must be clear and transparent on the purpose to which the data is to be used.

GSMA Commitment

GSMA is aware that the issue of handset theft cannot be effectively tackled on a country by country basis. A coherent regional policy is required in markets where handset theft and IMEI reprogramming is an issue to collectively and effectively address these challenges.

GSMA is committed to support the efforts of all stakeholders and can make a positive contribution in the following ways:

- Provide relevant and timely information to encourage increased use of IMEI blocking and the IMEI Database
- Work with network operators to agree and establish stolen handset data sharing rules in the form of a memorandum of understanding to ensure consistency of implementation within and across markets
- Encourage handset manufacturers to continue to innovate in the area of IMEI security and lobby additional handset manufacturers to join the security initiatives
- Monitor and enhance IMEI Database functionality required by members and national authorities to facilitate the international sharing of handset data
- Progress work with various stakeholders on complementary activities to disrupt the black market
- Continue collaborative approach with manufacturers, law enforcement agencies and governments

Proposed Next Steps

GSMA is willing to engage and dialogue with regulators, manufacturers and network operators to find solutions to the handset theft problem that can be universally applied. It is important that any measures to combat handset theft must be effective, efficient and cost effective to deploy.

GSMA believes the following steps and commitment are critical to combatting handset theft across the Americas:

- Network operators should deploy EIRs on their networks and commit to block handsets from accessing their networks

- Individual network EIRs should be connected to GSMA's IMEI Database to ensure stolen handset data is exchanged across the region
- Importers and purchasers of handsets should ensure the handsets they source comply with the technical security principles to ensure IMEIs cannot be changed to circumvent blacklisting
- Network operators to report instances where they become aware that IMEI security implementations have been compromised in specific devices in order that GSMA can refer the problem to relevant device manufacturers
- National authorities should support and encourage the licensed network operators in their jurisdictions to connect to the IMEI Database
- Governments should introduce legislation to criminalise the unauthorized changing of IMEIs and the supply or possession of equipment to undertake this activity
- All stakeholders should engage with GSMA to ensure the smooth implementation of the above initiatives

Annex A: Benefits of connecting to GSMA's IMEI Database

The global IMEI Database that is hosted by GSMA is a facility for mobile network operators to share stolen handset data on a national, regional and global basis. The platform is maintained by GSMA and is available for use free of charge. The Database allows operators to upload the details of mobile devices stolen from their subscribers and that data is made available for download to all other operators that are connected to the Database. This allows operators in any particular country to easily access the data submitted by network operators in their own country and in any range of other countries that they desire. This flexibility means that the GSMA's IMEI database is uniquely placed as a facility to host national, regional and international stolen handset registries without the operators or individual countries and regions having to develop their own databases. The GSMA already provides this functionality to operators in a number of countries.

Essentially, this means that all the operators in a particular country or region have to do is to connect their EIRs to the CEIR where they will have exclusive access to that country/region's directories to where they can upload and download data. The GSMA can work collectively with the operators in any region or country as the most efficient use of CEIR is for all operators to connect to the facility and to share data through a regional or national database.

Some of the benefits of using the CEIR can be summarized as follows:

- The IMEI Database is hosted by GSMA, which is an independent not for profit trade organization that represents the industry on a global level;
- The IMEI Database is provided for use by all network operators and does not incur any usage charges as it is offered as a service to the industry;
- The IMEI Database was developed to cater specifically for the needs of the industry to exchange stolen hands data;
- The IMEI Database is a stable technology that has been in existence since 1996. Significant investment in recent years has added to the functionality of the application to ensure it continues to meet current needs;
- The IMEI Database file formats, data interchange procedures, tests etc. have been defined by GSMA and its members and are available to implement without delay;
- The IMEI Database facilitates the upload and download of data by a variety of methods and at a variety of times depending on the needs of the users;
- The IMEI Database is entirely flexible in terms of how data is shared so national, regional and global sharing is fully supported;
- The IMEI Database offers the best option to ensure there is a maximum sharing of data across all operators as a number are already connected making it the most widely used stolen device data sharing tool;
- Connection to the IMEI Database is supported by all current EIRs in the marketplace so connectivity can be easily achieved.

Annex B: Handset Security Principles

In order to enhance IMEI security levels the industry agreed a set of nine handset security principles to provide guidance to handset manufacturers and to provide operators with a set of high level criteria against which handset security can be assessed. The following handset security principles are provided to help manufactures develop a comprehensive security architecture that facilitates the deployment of a range of solutions to protect the platform on which IMEI mechanism is stored.

1. Secure uploading, downloading and storage of executable code and sensitive data related to the IMEI implementation

2. Protection of components' executable code and sensitive data related to the IMEI implementation

3. Protection against exchange of data/software between devices

4. Protection of executable code and sensitive data related to the IMEI implementation from external attacks

5. Prevention of download of a previous software version

6. Detection of, and response to, unauthorised tampering

7. Software quality measures

8. Hidden menus should not have the ability to access or modify executable code or sensitive data

9. Prevention of substitution of hardware components

Annex C: Device Manufacturers Supporting IMEI Security Initiatives

The following device manufacturers have formally signed bilateral contracts to ensure the IMREI implementations in devices placed in the market by them meet the requirements set out in Annex B. They have also formally committed to participate in the IMEI security failure reporting and correction process.

- Alcatel
- Apple
- BenQ
- Enfora
- INQ
- Huawei
- LG Electronics
- Mitsubishi
- Motorola
- NEC
- Nokia
- Palm
- Panasonic
- Philips
- Sagem
- Sanyo
- Samsung
- Sharp
- Sony Ericsson
- Wavecom
- ZTE

Annex D: IMEI Database Basic Operation