Mobile Device Crime Data

Third Party Access Policy

Version 10.0
November 2018

1. Introduction

The GSMA fully recognises that mobile device crime is a major issue of public policy concern for network operators, consumers and regulatory authorities. To meet the challenges posed by increased media and regulatory attention GSMA is committed to support and enhance the provision of device data sharing services and to collaborate with stakeholders to demonstrate the industry's ability to work together to combat device crime.

In parallel with working with device manufacturers to improve IMEI integrity, GSMA is committed to provide and offer the functionality needed to allow parties other than Contributor Network Operators (CNOs) to access mobile device crime data exchanged through GSMA pursuant to SG.18 IMEI Database File Format Specification ("MDCD" or "Mobile Device Crime Data"). GSMA continues to invest in system and functional enhancements designed to meet the needs of a range of stakeholders.

2. Holistic Approach to Combatting Device Crime

The GSMA's activities to combat device crime are grounded in a commitment to initiate and implement a range of solutions that contribute to fighting this problem. The GSMA is fully aware of the increased level of international criminal activity related to device crime, which has resulted in the emergence of a black market for mobile devices in many jurisdictions.

Connectivity of network operator device blocking systems (e.g. EIR) to the GSMA IMEI Database ("IMEI Database") to exchange MDCD for pan-network device blocking is one such solution and is preferable to isolated and fragmented solutions that are of less value. Additionally, it is critical that other parties that have an interest in combating device crime can engage fully to implement appropriate crime prevention measures. Specifically, the GSMA seeks to encourage the following:

- Implementation, by device manufacturers, of the industry agreed technical principles to prevent the changing of device IMEIs
- Use of the industry initiated IMEI reporting and correction process by device manufacturers and operators to report and correct identified IMEI security weaknesses
- Introduction and enforcement of specific legislation by national regulators/governments to criminalize the unauthorised reprogramming of IMEIs
- Tools and services that identify devices with IMEI changes in cases where device design and legislation attempts to prevent this, have failed

It is hoped that a holistic range of measures, such as those listed above, will complement the connectivity of network operators to the IMEI Database, and greatly enhance the value of each of the other measures in an effort to reduce device theft and fraud related crime.

3. Third Party Access to Mobile Device Crime Data

Whilst network operators, manufacturers, enterprise customers and consumers are the most obvious stakeholders in the fight against device crime, there are a number of additional sectors that have a role to play and these include the following:

- Law enforcement agencies are in the front line of combating street crime and other aspects of criminal activity related to device crime
- Service repair centres that could be used, willingly or unknowingly, as clearing houses to launder devices by facilitating unauthorised IMEI re-programming
- Authorised dealers and retail outlets that exchange devices that have been purposely damaged to claim replacement devices under warranty programmes
- Insurance providers that underwrite device theft insurance policies provided to consumers
- Recyclers that could be used to launder criminally obtained devices by paying money to have the devices reused in other markets or have them broken up for parts
- Data aggregators that compile device data from a variety of sources to provide IMEI checking services to a range of stakeholders
- Industry organisations engaged in anti-fraud and anti-theft initiatives where the information would be of statistical interest
- Providers of solutions to help identify or prevent use of lost/stolen devices

This policy enables read only access to MDCD for parties other than network operators. It is believed that such third party access supports the holistic approach required to combat device crime.

4. Law Enforcement Access to Mobile Device Crime Data

Although there are many parties that could be interested in accessing device data, initiatives are underway in a number of jurisdictions to further engage law enforcement agencies in the fight against device related crime.

Permitting law enforcement read access to MDCD, in addition to demonstrating the industry’s willingness to support their efforts to investigate and prosecute device crime, ensures that a status, albeit not necessarily guaranteed, can be provided on IMEIs contained in the IMEI Database. This provides assistance to police investigations, particularly where devices have been specifically blacklisted in the GSMA IMEI Database.

5. Policy to Provide Third Party Access to Mobile Device Crime Data

Responsibility for formulation of the policy pertaining to third party read only access to MDCD rests with the GSMA's members and compliance with that policy is enforced by the GSMA support staff. Granting MDCD access by GSMA to third parties is only permitted in accordance with recommendations and procedures set down by GSMA members and approved by GSMA's Fraud and Security Group.

The policy set out in this document defines how best, and in what circumstances, MDCD can be made available to parties other than network operators. The GSMA IMEI Database supports multiple tiers of read only access to MDCD provided to third parties utilising the GSMA Device Check service.

5.1 Data Protection

Although there is no globally applicable data protection law as such, legislation has been enacted by individual countries based on similar high-level objectives. Unfortunately, this has culminated in different legislative provisions across individual countries and legal jurisdictions.

Different national requirements have to be considered and the priority of GSMA is to maximise operator use of, and data contribution to, the IMEI Database. GSMA's solution allows operators join the system safe in the knowledge that their data is partitioned in a manner that can prevent others from accessing it and to avoid conflict with national data protection regulations.

Although IMEI data on its own is generally not considered to constitute personal data, GSMA can assist operators connecting to the GSMA IMEI Database that may be compelled by local regulations to prevent the sharing of MDCD by allowing each operator the option to exclude their input from the dataset made available to third parties. This ensures that operators that are not under such constraints will have their data shared with the widest possible audience committed to combating device crime whilst those that are constrained can still use the GSMA IMEI Database in the knowledge that they do not breach local legal requirements.

This approach generally ensures the removal of any regulatory obstacles to operators intending to use the IMEI Database. This overall solution enables unconstrained operators to meet police demands while the GSMA works with those affected by more stringent requirements to better understand, and negotiate, the terms under which MDCD is used.

5.2 Liability

The GSMA, although the custodian of MDCD, is merely a provider of a centralised hosting service and does not own the data. Therefore, the GSMA cannot claim any responsibility for the accuracy or currency of the data it maintains. Appropriate disclaimers are in place to protect GSMA, and the operators that write to the GSMA Black List, to protect them against any claims that may arise as a direct result of action taken by any party because of information received from the GSMA IMEI Database. Such disclaimers are supported and complemented with appropriate confidentiality and restricted usage agreements that must be signed by third parties, clearly setting out the rights and obligations of those parties and absolving GSMA and CNOs from liability.

5.3 Classification of Third Party Access to Mobile Device Crime Data

A number of third parties require read only access to MDCD and access rights for each category of user, and the nature of the data to be accessible to each, is clearly defined. Five tiers, or levels, of third party access govern access to MDCD. These can be summarised as follows;

Third Party User Classification	User Description
Third Party A	Law enforcement and customs agencies Regulatory bodies
Third Party B	National / Regional Interest groups
Third Party C	Commercial entities • Authorised Dealers • Repair and refurbishment centres • Providers of device insurance, warranty and financing services • Recyclers and traders of used devices • Providers of reverse logistics services and solutions • Device manufacturers • Mobile Virtual Network Operator (MVNO) • Providers of solutions to help identify or prevent use of lost/stolen devices
Third Party D	General Public
Third Party E	IMEI Checking Service Providers. Entities that provide IMEI checking services to eligible end-users, as defined in in this document as Third Party A, B C or D, including through another IMEI Checking Service Provider.

5.4 Nature of Data to be Disclosed

GSMA members have clearly defined the type of data to which third parties have read only access. In all cases, the input is a single IMEI number, via the GSMA Device Check service, and the following table sets out the nature of data that may be returned in response to queries originated by types of third party end-users;

Third Party User Classification	User Description	IMEI Database Output in Response to Third Party Query
Third Party A	Law enforcement and customs agencies Regulatory bodies	• Whether or not the input IMEI is present on the Black List • Date of each Black List entry for that IMEI • The CNO, and corresponding country, responsible for each Black List entry for that IMEI • If TAC information exists for that IMEI, the manufacturer and marketing name of the device • Crime reference number (where available)
Third Party B	National / Regional Industry Interest groups	• Whether or not the input IMEI is present on the Black List • Date of each Black List entry for that IMEI • The CNO, and corresponding country, responsible for each Black List entry for that IMEI • If TAC information exists for that IMEI, the manufacturer and marketing name of the device
Third Party C	Commercial entities	• Whether or not the input IMEI is present on the Black List • Date of each Black List entry for that IMEI • The CNO, and corresponding country, responsible for each Black List entry for that IMEI

		• If TAC information exists for that IMEI, the manufacturer and marketing name of the device
Third Party D	General Public	• Whether or not the input IMEI is present on the Black List • If TAC information exists for that IMEI, the manufacturer and marketing name of the device
Third Party E	IMEI Checking Service Providers	• Whether or not the input IMEI is present on the Black List • Date of each Black List entry for that IMEI • The CNO, and corresponding country, responsible for each Black List entry for that IMEI • Crime reference number (where available) • If TAC information exists for that IMEI, the manufacturer and marketing name of the device The above information is available to IMEI checking service providers in so far as the data may only be provided to others according to the applicable Third Party classification.

Notes:

1. A crime reference number is made available to law enforcement agencies to assist them with their investigations where connected operators have the capability to capture the necessary data and upload it in their records by using the otherwise redundant “Comments” field.
2. The Type Allocation Code (TAC) agreement between GSMA and device manufacturers provides GSMA the ability to disclose device detail information as appropriate and to be of benefit to the industry. Such information, much of which is exchanged through the IMEI Database, is not classified as Mobile Device Crime Data but is useful in providing clarity and authenticity of mobile devices. Examples of such information include manufacturer, make/model, device type, and networking capabilities.

5.5 Third Party Access Approval

Third party access is controlled and monitored and each organisation accessing MDCD has a named GSMA Device Check account established to which unique user credentials are allocated after completion of appropriate registration procedures. An appropriate end user Agreement must be signed and submitted to GSMA before applications are processed.

GSMA support staff takes responsibility for vetting the bona fides of each applicant and its eligibility to access data as an eligible third party as defined in Section 5.3. All checks are thoroughly undertaken by GSMA staff, which take and retain the applicant’s details and the evidence supporting its application for review by any GSMA member that may wish to do so.

If GSMA staff are unable to fully satisfy themselves as to the eligibility or bona fides of an applicant they may seek the assistance of any CNO. In the event that such CNO assistance is necessary, the following table sets out the support and sponsorship criteria that must be satisfied for each category of user that applies from a jurisdiction in which there are one or more CNOs.

Third Party User Classification	User Description	Sponsorship Required
Third Party A	Law enforcement agencies Regulatory bodies	- Sponsorship letters from at least two[1] IMEI Database connected operators in the jurisdiction where the applicant police force has authority - Sponsorship letter from all of the CNOs in the relevant jurisdiction in the case of a regulatory body
Third Party B	National / Regional Interest groups	- Sponsorship letters from at least two CNOs in the case of national /regional interest groups
Third Party C	Commercial entities	- Sponsorship letter from a CNO, except for a GSMA member device manufacturer in which case approval may be obtained from the GSMA Head of Fraud and Security.
Third Party D	General Public	- Not applicable
Third Party E	IMEI Checking Service Provider	- Sponsorship letters from at least two CNOs

Appropriate application forms and sponsorship letters will be provided by GSMA to support the processing of applications for third party read access to MDCD.

In the case where a request is received from a third party in a jurisdiction in which there are no CNOs, GSMA staff will seek to vet the bona fides of the applicant and assess its eligibility to access data as it would do for an applicant from a jurisdiction in which there is at least one CNO. If GSMA staff are unable to fully satisfy themselves as to the eligibility or bona fides of an applicant they may seek the assistance of any local operator(s), regardless of their status as a CNO.

Approved Third Parties are listed within the GSMA IMEI Database for the information of IMEI Database users.

5.6 IMEI Checking Service Provider Access

Similar to other Third Parties, IMEI Checking Service Providers are permitted read-only access to the GSMA IMEI Database using both web and API interfaces. Additionally, for a limited period extending to no later than 31st March 2019, GSMA will support parties that have been receiving the data as a file download, during which time such parties will migrate to the API mechanism.

[1] Where there is only one operator in that jurisdiction, or where there is only one CNO, the authority of that single operator will be sufficient. In cases where there are no CNOs from that jurisdiction, access can be granted following consultation with any local operator(s) that can assist the vetting process.

6. Funding of Third Party Access to Mobile Device Crime Data

It is not the intention of GSMA to profit from the problem of device crime but it is necessary to levy some charges in order to recoup development, operational and associated costs. Fees applicable to the GSMA Device Check service are available from GSMA and apply to commercial organisations as the service is provided free of charge for law enforcement agencies and regulatory bodies strictly as end-users.

7. Conclusions

Third party read only access constitutes a significant initiative on the part of GSMA and its members to enable other organisations, and consumers, to combat device fraud and theft related crime. GSMA is pleased to offer the facility to qualified parties and it is willing to provide eligible applicants with the support necessary to obtain access to MDCD in accordance with the GSMA approved policy.