



GSMA guidelines on the protection of privacy in the use of mobile phone data for responding to the Ebola outbreak

October 2014



Introduction

When Call Data Records (CDRs) are used to help in the response to the Ebola outbreak, mobile operators wish to ensure mobile users' privacy is respected and protected and any associated risks are addressed. This document outlines, in broad terms, the privacy standards that mobile operators will apply when subscriber mobile phone data is used, in these exceptional circumstances, for responses to the Ebola outbreak.

GSMA guidelines on protecting privacy in the use of mobile phone data for responding to the Ebola outbreak

Mobile operators will anonymise CDRs and adopt robust technical and organisational measures to protect them against unauthorised access and use. The analysis of the anonymised records by third parties (including research agencies, aid agencies and governments) and the sharing of any output from the analysis will take place under legal contract(s) based on this document.

Specifically,

1. The mobile phone numbers of subscribers making and receiving calls or text messages will be anonymised by mobile operators inside their premises and on their equipment. This is achieved by replacing the mobile phone numbers with an anonymous code before being analysed. This is done through a hashing process using the secure SHA-3 algorithm¹.
2. Anonymised CDR data will not be transferred outside of the operator's system/premises: The anonymised data will be kept secure and encrypted within the operator's premises. Access to the data will be controlled and given only to pre-approved and authorised personnel. A record of access will be maintained and auditable. Access to the algorithm and the ability to decrypt the data will be further protected by also limiting access to pre-approved and authorised personnel.
3. All analysis will take place on mobile operator's systems, in their premises and under operator supervision. Once anonymised by the mobile operator, the data will be analysed by approved research entities that agree to abide by strict ethical standards on the use of data.
4. No analysis will be undertaken that singles out identifiable individuals. No attempts will be made to link the data to other data about an individual and which may impact on their privacy or otherwise cause harm.
5. Only the output of the analysis (i.e. the resulting non-sensitive data on population mobility estimates, aggregate statistics, indicators, etc.) will be made available to relevant and approved aid agencies, government or research agencies that can use these inputs in their modelling and planning efforts. No sensitive data will be shared with or made available to any third parties.

Annex – Definitions

- *Call Detail Records (CDR) data* – a record of a voice call or an SMS generated by a mobile network operator that includes the mobile number of both the person making and receiving the call, date, time and call duration, and low resolution location information (nearest cell tower).
- *Anonymised CDR* – the data above with personal information (such as mobile number and subscriber information) de-identified.
- *Mobility estimates* – aggregate population mobility statistics based on the analysis of anonymised CDR data, and that does not contain any personal or otherwise sensitive information.

¹ <https://en.wikipedia.org/wiki/SHA-3>