# Draft Code of Conduct for Third-Party Use of Big Data Generated by Mobile Network Operators

Rohan Samarajiva

Negombo, August 2014


IDRC CRDI
Canada

This work was carried out with the aid of a grant from the International Development Research Centre, Canada and the Department for International Development UK..

UKaid
from the British people

# Purpose

- Reduce transaction costs of releasing mobile network big data (MNBD) to third parties for public and commercial purposes

*First step in a process that will hopefully lead to the adoption of a voluntary code of conduct by the region's mobile network operators (MNOs) that will be the most effective in minimizing possible harms*

# Method

- Potential harms have been identified through
  - the literature (Annex 1) and
  - engagement with ongoing analysis of MNBD at LIRNE*asia*

*Anchored on my work on utility transaction-generated data since 1991*

# Definitions

- Big data: data that are very large in volume, diverse in variety and/or moving with such velocity (3 Vs), that traditional modes of data capture and analysis are insufficient and the insights generated therefrom are qualitatively more valuable
- MNBD include, but are not limited to
  - Call Detail Records of CDRs (associated with voice calls, SMS and data use)
  - Visitor Location Register (VLR) data used to locate mobile devices in use (collected but rarely stored)
  - Reload data applicable to prepaid customers
  - Additional data such as GPS [Global Positioning System] and some app generated data in case of smartphones
  - Data from certain apps such as Google and Facebook not included

# One classification, based on actions related to processing

| | Real time | Historical |
|---|---|---|
| **Identifiable** | RTI | HI |
| **Anonymized** | RTA | HA |

# Considered harms

- Privacy (9 out 16)
  - Surveillance
  - Aggregation
  - Identification, individual and group
  - Insecurity
  - Secondary use
  - Exclusion
  - Breach of confidentiality
  - Disclosure
  - Increased accessibility
- Anti-competitive effects
- Marginalization

| Remedy | Identified potential harm | Include in agreements transferring identifiable MNBD | Include in agreements transferring anonymized MNBD |
|---|---|---|---|
| Mobile Network Operators (MNOs) will not engage in active surveillance of their customers, except as required by applicable law. MNOs will desist from collecting more data than are needed for the efficient operation of the networks and the supply of good service to customers. To the extent feasible, data collection practices will be transparent. | ***Active surveillance*** | No. Applying only to MNOs, this need not be included in agreements. However, active surveillance is a root cause of problems that could be manifested in other forms at the subsequent information processing and dissemination phases. | No. Applying only to MNOs, this need not be included in agreements. However, active surveillance is a root cause of problems that could be manifested in other forms at the subsequent information processing and dissemination phases. |

| Remedy | Identified potential harm | transferring identifiable MNBD | anonymized MNBD |
|---|---|---|---|
| anonymization. | ***De-anonymization*** | No | Yes |

| Remedy | Identified potential harm | Include in agreements identifiable MNBD | Include in agreements anonymized MNBD |
|---|---|---|---|
| Individually identifiable data will not be released to third parties, unless the purposes are specified in the agreement and have been approved by an ethics review committee, if one is available. If an ethics review committee is not available, an equivalent third-party | ***Individual identification*** | Yes | No |

| Remedy | Identified potential harm | Include in agreements transferring identifiable MNBD | Include in agreements transferring |
|---|---|---|---|
| Any agreement transferring identifiable data to a third party will also transfer responsibility to maintain safeguards to ensure security of individually identifiable data. | ***Insecurity*** | Yes | No |

| Remedy | Identified potential harm | Include in agreements identified in MNBD | Include in agreements |
|---|---|---|---|
| The agreement governing the transfer will include provisions to minimize risks posed by increased accessibility when data are released to third parties. | ***Increased accessibility*** | | Yes |

| Remedy | potential harm | transferring identifiable MNBD | transferring anonymized MNBD |
|---|---|---|---|
| accommodation for | ***Anti-competitive effects*** | Yes | Yes |